

Conference Proceedings of

***Ai*CE 2008**

Melbourne, 11 February, 2008.

**Fifth AUSTRALIAN INSTITUTE OF
COMPUTER ETHICS CONFERENCE**



**Edited by:
Matthew Warren
ISBN 978-1-74156-100-5**

Proceedings of

AiCE 2008

Edited by

Matthew Warren

ISBN 978-1-74156-100-5

Organised By

National Security Research Group,
Faculty of Business and Law,
Deakin University.

Published by the School of Information Systems, Deakin University,
Burwood, Victoria, 3125, Australia.

All papers published in the conference proceedings have been blind
refereed by at least two of the AiCE 2008 **Organising and Review**
committee.

© Deakin University, 2008.

Welcome

The AiCE208 conference follows on from the highly successful initial AICEC99, AICE2000, AICE2002 and AICE2005 conferences. This conference looks at the continued development of Computer Ethics within Australia, taking into account the current issues that impact Australia.

Members of the conference organising committee accepted each paper in the proceedings after a careful review; this took the form of a **blind review** by at least **two** members of the conference organising committee. The papers were subsequently reviewed and developed where appropriate; taking into accounts the comments of the reviewers. The aim of this conference is to further the work already achieved within Australia and bring together researchers in the field to discuss the latest issues and their implications upon Australia.

We commend the authors for their hard work and sharing their results, and the reviewers of the conference for producing an excellent program.

AiCE 2008 Organising Committee

John Barlow, Australian Catholic University.

William Hutchinson, Edith Cowan University.

Oliver Burmeister, Swinburne University.

Matthew Warren, Deakin University. (Conference Chair).

John Weckert, Charles Sturt University.

Shona Leitch, Deakin University.

Contents

Page Number

A Survey of Ethics and Regulation within the ICT Industry in Australia: Ethics Education R Lucas and J Weckert.	1
The Reasonable Adult and Community Standards G A Sandy.	10
The Ethics of Compulsory Open Source J Thomson.	18
Expanding the IT Territory: Creating Space for Ethical IT I Stoodley and C Bruce.	24
The Gamer's Dilemma, M Luck.	31
Critical perspective on Ambient Intelligence technology - ethical and societal issues P Goujon.	32
Ethics for IT: A short Weberian excursus D Coulthard.	57
The Ethics of Information Operations, W Hutchinson.	63
Ambient technology: Reconsidering informed consent P Duquenoy and O K Burmeister.	68
Encouraging Ethical Decision Making in Security Policies A B Ruighaver.	79
Developing professional ethics through game design and role-play with the Pirate's code of conduct K Eustace.	80
A Theoretical Framework for Academic Integrity K Fielden.	90
Scandal, Censorship and Representation in the Online World: An Ethical Conundrum G Pye and A Miller.	98
Virtual World, Real Ethics: Challenges for Online Counselling R Andary and D A Banks.	105

The Wikipedia: Experts, Expertise and Ethical Challenges S Lichtenstein.	112
Security and Ethical Issues in the Virtual World of Second Life C Y Lee.	119
Designing Ethical Systems for Online Systems S Leitch and M J Warren.	130
Young People and the Internet - What is the solution? S Leitch and M J Warren.	137

A Survey of Ethics and Regulation within the ICT Industry in Australia: Ethics Education

Dr. Richard Lucas
Centre for Applied Philosophy and Public Ethics
Australian National University
LPO Box 8260, Canberra ACT, 2601, Australia
Telephone: +61 2 6125 8469
Email: Richard.Lucas@anu.edu.au

Prof. John Weckert
Centre for Applied Philosophy and Public Ethics
Charles Sturt University
Telephone: +61 2 612 58995
Email: jweckert@csu.edu.au

ABSTRACT

Presented here is a preliminary analysis of ethics education across a number of demographic and substantive questions asked in a survey of ethical attitudes of professionals in the ICT industry in Australia.

For general tertiary education, only three-quarters of the respondents had any at all. Within these less than half reported having had any formal ethics education. Also more than one-third said that their ethics education was not helpful.

It was found that there was a significant difference between what the tertiary institutions claim to deliver by way of ethics education, what the ACS demands, and what the respondents said they received. It was also found that the quality of the ethics education the respondents received was poor.

INTRODUCTION

Education is the foundation of understood and repeatable ethical decisions and behaviour. For this reason we examined the state of ethics education of our respondents.

Here we report on the questions that asked about ethics education of a survey that examined the beliefs of ICT professionals concerning the state of ethical behaviour and regulations in Australia. In this paper we will focus on the responses given to the questions about ethics education across a number of demographic and substantive questions.

THE SURVEY

We asked three questions concerning the respondents' ethics education.

ETHICS EDUCATION of ICT workers. That is what is the nature of ethical education that ICT professionals received.

Q.29 If **yes** → Q.31

Q.30

Q.29 Have you had any formal ethics training or education? [Yes, No, Unsure]

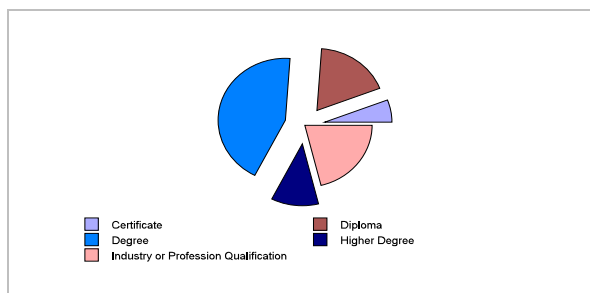
Q.30 Everyone has had some sort of informal ethical education. If there is there any specific education of this kind that you would like to mention do so here. An example might be moral education from a religious or secular group.

Q.31 If you answered yes to question 29 do you think it would help in responding to situations in which unethical behaviour might occur?
[Yes, No, Depends, Unsure]

SURVEY RESULTS

Individual Question Results

By way of placing the discussion of tertiary ethics education the following background data is relevant.



Just over three-quarters (76.7%) of the respondents had some form of ICT tertiary qualification. Of those, almost all (96.7%) listed their qualifications with an average of 1.25 qualifications per respondent.

Figure 1 - Tertiary Qualifications

Question 29. Have you had any formal ethics training or education?

Question 29. Have you had any formal ethics training or education?		
Response	Number of Responses	Percent of Total Responses
Answered	348	98.3%
Did Not Answer	6	1.7%
Total	354	Percent of Answered Responses
Yes	156	44.8%
No	182	52.3%
Unsure	10	2.9%

That only 44.8% said yes seems to be at odds with the fact that 37 of 38 Australian universities are accredited by the ACS which has as a mandatory component an ethics module.

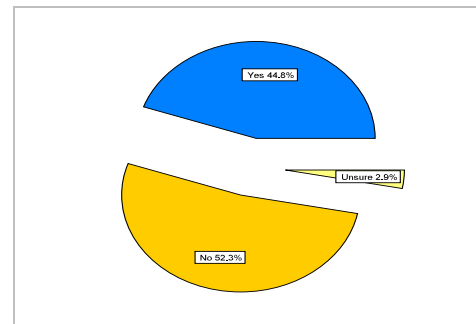


Figure 2 - Formal Ethics Education

Question 30. Everyone has had some sort of informal ethical education. If there is there any specific education of this kind that you would like to mention do so here. An example might be moral education from a religious or secular group.

Question 30. Everyone has had some sort of informal ethical education. If there is there any specific education of this kind that you would like to mention do so here. An example might be moral education from a religious or secular group.			
Response	Number of Responses	Percent of Total Responses	
Answered	178	50.3%	
Did Not Answer	176	49.7%	
Total	354		
	Modes of Training	Percent Within Kind	Percent Within All Responses
Formal			
Lecture	6	8.1%	3.0%
Module	8	10.8%	4.1%
Seminar	7	9.5%	3.6%
Subject	30	40.5%	15.2%
Tutorial	1	1.4%	0.5%
Work Organized	18	24.3%	9.1%
Profession Organized	4	5.4%	2.0%
SubTotal	74		37.6%
Informal			
Culture	4	3.3%	2.0%
Faith	54	43.9%	27.4%
Family	20	16.3%	10.2%
Role Model	2	1.6%	1.0%
Scouts	2	1.6%	1.0%
Self-study	41	33.3%	20.8%
SubTotal	123		62.4%
Total	197	100.0%	100.0%

Most of the 178 who gave detailed answers included extensively explained multiple examples. Only the coded table of responses is included here.

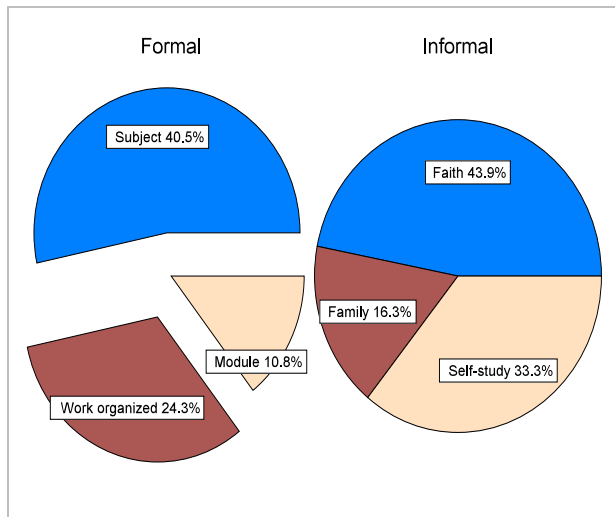


Figure 3 - Kinds of Ethics Education

We then pointed out that all people have had some form of informal training and asked if respondents would tell us about any form of ethical training or education. More than half replied (this is more than those who said they had formal ethics education) and of those 37.6% listed some kind of formal training (lecture, work, etc.) while 62.4% listed some kind of informal training. Of the 62.4% informal training or education, faith was the most common (43.9%). This was followed by self-study (33.3%) and family (16.3%). Other lesser kinds were culture, a role-model, and Scouts. Clearly the education system is not preparing these respondents for encountering unethical behaviour in the workplace. It seems that they rely more on their own devices than the education system.

Question 31. If you answered yes to the previous question do you think it would help in responding to situations in which unethical behaviour might occur?

Question 31. If you answered yes to question 29 do you think it would help in responding to situations in which unethical behaviour might occur?		
Response	Number of Responses	Percent of Total Responses
Answered	227	64.1%
Did Not Answer	127	35.9%
Total	354	Percent of Answered Responses
Yes	141	62.1%
No	27	11.9%
Depends	45	19.8%
Unsure	14	6.2%

Why should only 62.1% of respondents indicating that their education in ethics was of any help?

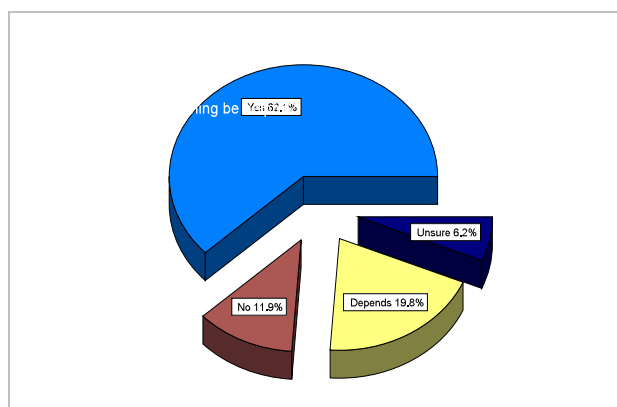


Figure 4 - Ethics Training Helpfulness

We then cross-tabulated the answers to the above questions with a number of demographic and substantive questions.

We looked at the respondents' ethics the demographic questions concerning AGE, GENDER, EDUCATION-TECHNICAL, and LOCATION. We also examined ethics education across the substantive questions relating to AWARENESS, REGULATION, and ACTION-TAKING.

GENERATION

Here we wanted to know if there was a generational difference in the formal education about ethics that the respondents received. As the number of unsure responses was very small for all generations (zero in some cases), they have been excluded from this analysis.

There were significant differences between the generations. Gen Y had the closest result; nearly equal numbers of yes and no (it had a difference of 1 between the yes and no responses). In contrast, the Baby Boomers and Gen X had significantly fewer saying yes than no. Depression – WWII Babies and Gen Jones were the only generations to record a greater number of yes than no replies. There is no apparent trend or generational bias in the formal education concerning ethics. We would have expected Gen Y to have more ethics education but they did not. Like so much of the results from Gen Y this is in need of further research.

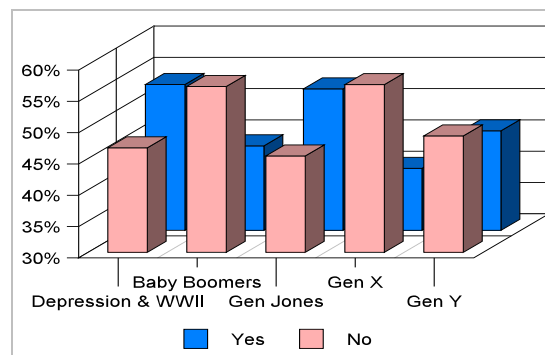
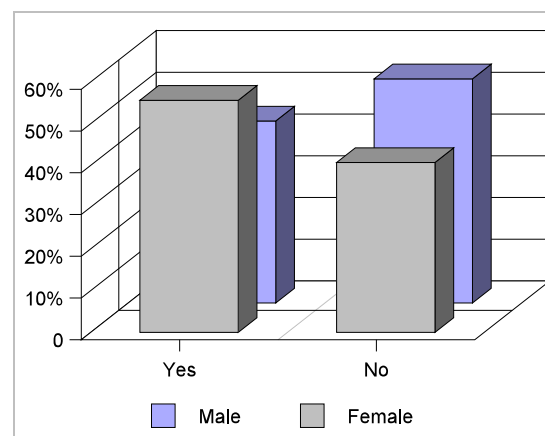


Figure 5 - Generational Ethics Education

GENDER

While there was a statistically significant difference between the genders when it came to their education/training about ethics neither was nearly as high as it ought to be. Females reported more ethical education (53.6%) compared to males (43.6%). Are females rather than males more inclined to take an ethics elective? Unfortunately we did not ask if the formal ethics education that respondents received was compulsory or an elective.



EDUCATION-TECHNICAL

We wanted to know of those with ICT specific qualifications whether they had any formal ethics education. While more than half of those who said they had ICT specific qualifications said they had no formal ethics training or education and less than half for those without, the difference between those with and those without ICT specific qualifications was not statistically significant.

LOCATION

There was no significant difference between capital city and regional centre respondents concerning their ethics education. Both had less than half of the respondents saying that they had any formal ethics education.

ETHICAL AWARENESS

While those who said they received no formal ethical education felt slightly stronger about how often unethical behaviour occurs, the difference was not statistically significant. There was no significant difference (mean of 3.43 vs 3.47, with occasionally = 3 and frequently = 4) between those with ethics education and those without, with both seeing unethical behaviour as mostly occurring between occasionally and frequently in the industry.

REGULATION

We wanted to know if having any ethics education made any difference to three things concerning regulations surrounding ICT ethics: knowledge of ethics regulations at work and if so, did they think they were effective, and finally were personal ethics sufficient for ethical problems at work.

On the first two questions there was no statistically significant difference between those with and those without formal ethics education. The result of the first was unexpected as it would, *prima facie*, seem that those with some formal ethics education ought to be more knowledgeable of ethics regulations at work simply by being more able to recognize them.

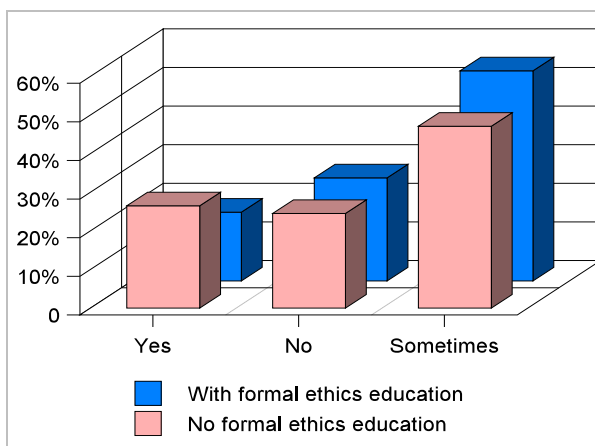


Figure 7 - Ethics Education and Personal Ethics

However, on the third question those who reported having some formal ethics education were less likely to say that personal ethics were sufficient.

This means that, for these respondents their ethics education made a difference to awareness of ethical problems but, as we see in the next section it makes no difference to their action taking.

ACTION-TAKING

We wanted to know if having any ethics education made any difference to whether the respondents would speak up over an unethical act. The two questions here are:

- ▶ would you speak up if you saw an unethical act and
- ▶ have you ever spoken up over an unethical act?

There was no statistically significant difference between those with and those without formal ethics education. The result of this was unexpected as it would, *prima facie*, seem that those with some formal ethics education ought to be more inclined (being armed with better tools for ethical discourse) to speak up. Is this even more evidence of the ineffectiveness of ethics education and training?

The final relationship we wanted to know about was for those with ethics education did they act unethically when asked to do so?

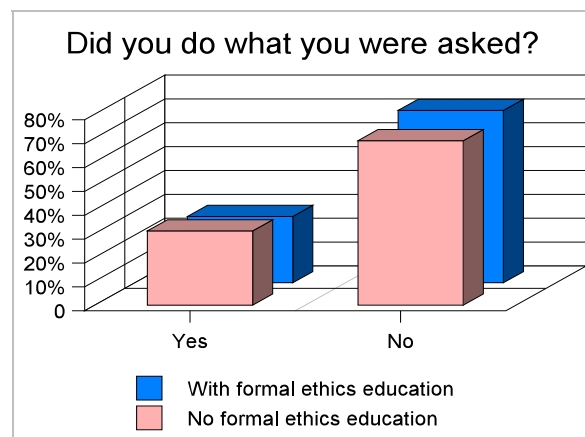


Figure 8 - Ethics Education and Acting Ethically

There was a slight difference with fewer of those with ethics education saying they did what they were told even when they knew it was unethical (27.8% did vs 31.1% did not).

DISCUSSION

This section discusses three issues relating to the ethics education of ICT professionals; educational mismatch, place of ethics in ITC curricula, and unqualified teaching personnel.

The survey suggests that formal qualifications in ICT did make a statistically significant difference in ethical behaviour in one area, unfortunately it was not in the direction that we would have preferred. Those with ICT qualifications were more likely to do what they were asked when approached to do something unethical. Why? One possible reason for this is that ICT education may be very narrow; it may be more that what is offered as ICT education is merely training rather than education.

Almost all of Australia's universities are accredited by the ACS and all courses accredited by the ACS must contain a component that studies the ethical and social issues related to ICT. In an internet examination of all university courses in Australia we found such components in all but two universities. One result of our survey however was that, in general, completing these components made no statistically significant difference to the ethical attitudes or behaviour of ICT professionals.

While the ACS does require the ethical component to be covered in order for a course to be accredited it does not require that there be a discrete subject; that it may be included as part of other subjects. From our search of ICT ethics offerings at Australian tertiary institutions it is clear that coverage by inclusion as a part of another subject is by far the most popular option. The fact that both methods are used reflects a debate regarding the best way of teaching ethics to ICT students. One school of thought is that there must be a discrete subject with rigorous assessment for students to take the issues seriously. The other view is that discussion of ethics should not be conducted separately because if it is then students do not see it as an integral part of the profession. A leading advocate of this view is Don Gotterbarn. He argues that ethics education is much more effective if it is incorporated throughout the curriculum rather than being taught as a discrete subject or course, and second, that it not necessarily best taught by philosophers or theologians. His concern is not to denigrate a philosophical approach to computer ethics but it is rather to understand how best to ethically educate computing professionals. A related debate, also mentioned by Gotterbarn, concerns the teachers of ethics; by what sort of person should it be taught? On the one hand it is argued that it should be taught by experts in ethics and on the other hand there are arguments for it being taught by ICT professionals because they know what the real issues are and they have more credibility in the eyes of the students. In both of these debates there are good arguments on both sides.

How do what the survey showed were the main ethical concerns compare with the typical content of accredited university courses and the contents of the most common texts used?

As could be expected, privacy and intellectual property issues were prominent but what could generally be described as professional issues, that is, issues where professionals must make work-related decisions, dominated. High on the list were compromising quality to meet deadlines, unprofessional behaviour, making false promises, and conflicts of interest. Also significant were compromising functionality and requirements to meet deadlines. Unprofessional behaviour also figured large in the extra comments section. Typical concerns were blaming others for one's own mistakes, poor team contributions, awarding contracts without due process, overpricing and under quoting of time and overstating of skills. The issue of professionalism was also of major concern in the interviews and most of the same worries surfaced. A number of related new ones were also mentioned, of particular significance were responsibility and informed consent.

A survey of the material covered in courses suggested that the common topics covered were the standard ones of privacy, security, cyber crime, intellectual property, regulating commerce and speech and a few others, with professional ethics being one topic but frequently left unspecified. The

most common text mentioned is Michael J. Quinn, *Ethics for the Information Age*, so a reasonable assumption is that the topics covered in the text also form the basis of the courses in which it is used. It's one chapter on professional ethics covers the issue of whether software engineering is a profession, the software engineering code of ethics, and codes of ethics in general, and whistle blowing. Notably, many of the issues raised in the survey and interviews are not explicitly mentioned either in this text or in the course descriptions. It does not necessarily follow from this that these topics are not covered but at least it raises the question of whether the focus of ethics courses is on the most important issues.

While the ACS does require the ethical component to be covered in order for a course to be accredited it does not require that there be a discrete subject and in most courses ethics is merely a part of other subjects. It is clear that this is by far the most popular option for universities. That there is this choice reflects a debate regarding the best way of teaching ethics to ICT students. One school of thought is that there must be a discrete subject with rigorous assessment for students to take the issues seriously. The other view is that discussion of ethics should not be conducted separately because then students do not see it as an integral part of the profession. A leading advocate of this view is Don Gotterbarn. He argues that ethics education is much more effective if it is incorporated throughout the curriculum rather than being taught as a discrete subject or course, and second, that it not necessarily best taught by philosophers or theologians. His concern is not to denigrate a philosophical approach to computer ethics but it is rather to understand how best to ethically educate computing professionals. A related debate, also mentioned by Gotterbarn, concerns the teaching of ethics; by what sort of person should it be taught? On the one hand it is argued that it should be taught by experts in ethics and on the other hand there are arguments for it being taught by ICT professionals because they know what the real issues are and they have more credibility in the eyes of the students. In both of these debates there are good arguments on both sides.

Three issues then have emerged from the survey and the literature: there appears to be a mismatch between what is taught and what professionals see as the most important ethical issues; there might be a problem with the place of ethics in ITC curricula and; it may not be taught by the most appropriate people.

CONCLUSION

The survey suggested that ethics education has no effect on ethical attitudes or on ethical behaviour. The survey and the interviews together with the internet examination of the content of courses, suggest that there may be a mismatch between what is taught and what the main issues really are for working professionals.

We have concluded from the survey that the ethics education of ICT professionals is deficient; that there is a serious mismatch between what the tertiary institutions claim to deliver by way of ethics education, what the respondents said they received, and what the major professional ICT body, the ACS, demands.

This leads to a series of questions which require further research to answer. Why is there such a poor correlation between general, technical, and ethical education? Why does ethics education seem to make little or no difference across a number of measures, including recognition of ethical problems and speaking up over unethical acts? What are the actual contents and delivery mechanisms used by tertiary institutes? What is the actual mechanism, and how effective is it, that the ACS uses to ensure that the claims tertiary institutes make for their ethics modules are actually being delivered, and done so effectively?

In particular we recommend that attention is given to three issues concerning the ethics components of ICT tertiary education; content, structure, and teachers.

Content. Professional issues, for example software quality issues, were of most concern to those surveyed and interviewed but most ethics courses seem to concentrate on social issues. Given this, it is reasonable to suggest that more emphasis should be placed on professional issues.

Structure. The internet survey of ICT courses showed that most did not have a discrete ethics subject, rather the required ethics component was part of one or more other subjects. While this is not necessarily a problem and is often seen as the best way of introducing students to the ethical problems, it can also be an excuse for not giving ethics a prominent place in the course. It can also suggest to students that, because there is no discrete subject with normal assessment requirements, ethics does not need to be taken seriously (we have seen an example where ethics was a component of a subject but where there were no assessment items for the ethics content). We believe that the most effective structure is to have a discrete ethics subject which is then complemented by assessable ethical reflection in other subjects. Where this is not done we recommend that ethics be integrated into other courses, and that the ethical content and assessment (when measured across all the subjects it appears in) be equivalent to a full subject.

Teachers. It is important that teachers of ethics have a good knowledge and understanding of both ICT and ethics. One possible reason for the lack of efficacy of ethics teaching in ICT courses is that those teaching it are competent in one but not the other, so that either what is taught is either not ethically rigorous or not relevant. An ICT professional without ethics training will flounder when challenged in class and an ethicist without a solid background in ICT will be found to be not believable, not have the right kinds of experience to relate their theory to actual practice. We recommend that institutions consider offering programs for teachers of computer ethics to supplement deficiencies in either area.

In summary, the ethics education of ICT professionals in Australia is in need of serious review and change.

The Reasonable Adult and Community Standards

Geoffrey A Sandy

School of Information Systems

Victoria University

Melbourne, Australia

Geoff.Sandy@vu.edu.au

Abstract

This paper addresses two key questions. First, who exercises the role of the reasonable adult and upholder of community standards regarding Internet content in Australia, and how is this exercised? Second, what are the major challenges to the efficacy of the current arrangements? It concludes there is probably a disconnect between actual community standards and what legislators and parliamentarians believe they are.

Keywords

Reasonable Adult, Community Standard, Internet Censorship.

INTRODUCTION

When classification decisions are made in Australia about Internet content appeal is made to the hypothetical entities of the “reasonable adult” and “generally accepted community standards”. The Office of Literature and Film Classification Guidelines for Films and Computer Games (OLFC 2005a) defines a reasonable adult as one “possessing common sense and an open mind, and able to balance personal opinion with generally accepted community standards”. The Guidelines assume that we all know what is meant by “common sense”, “open mind”, “personal opinion” and “generally accepted community standards” for these key terms are nowhere defined.

Classification decisions are made for two reasons. First, is the provision of consumer and publication advice about the nature of the content. Each classification category contain a list of criteria which are used when making decisions. Examples of a classification category are RC = Refused Classification, X = Restricted 18+ (films only) or R = Restricted 18+. Examples of criteria are violence, sex, drug use and nudity. Decisions account for individual elements and cumulative effect.

A second reason for classification is that it is required by the various Acts of the Federal and State and Territory parliaments. To illustrate, the relevant Federal legislation is the Broadcasting Services Amendment (Online Services) Act 1999 Internet content hosted onshore and classified RC is subject to a take down notice served on an Internet Service Provider (ISP). Indeed any offline as well as online content with RC is illegal. Again any Internet content hosted onshore classified X is subject to a take down notice and any content hosted onshore and classified R is subject to a take down notice unless subject to a Australian Communications and Media Authority (ACMA) approved verification system. The States and Territories all have legislation to regulate Internet content but it varies between the jurisdictions. A list of the relevant legislation is provided as Appendix A.

This paper is concerned with two key questions. First, who exercises the role of the reasonable adult and upholder of community standards regarding Internet content in Australia and how is this exercised? Second, what are the major challenges to the efficacy of the current arrangements? Given the permitted length for the paper it must necessarily be in summary form with most weight given to the second question. Similarly, most attention is given to the regulatory aspect rather than that of

consumer advice. Again most attention is given to the consumption rather than the production of Internet content.

The discussion will use the Internet content type generally referred to as pornography to illustrate. There are two reasons why this is a useful choice. First, community concerns about pornography have long been cited as a justification for its regulation offline. Those of this view argue that the need to regulate pornographic Internet content is even greater because of the ease with which the technology allows access to adults and minors, and, a belief that the Internet is “awash with pornography”. The main reason for the Online Services Act for instance, was to regulate pornography. It should be noted that the OLFC does not refer to pornography but does to “sexual content”, “sexual violence” and “nudity”. No attempt is made in this paper to define and classify pornography. That is worthy of a paper in its own right.

Second, how you treat pornography is a good test of the “openness” of that society. Pornography can be viewed as subversive and challenge the traditional institutions of church and state. Commonly it is viewed to be harmful with some types declared illegal, such as child pornography. Libertarians would overwhelmingly agree that the State is on safe grounds when justifying regulation of child pornography and where non consensual activity is involved. This is not the case for consensual activity. Research studies¹ overall do not support an explicit causal link between consuming the pornographic image and harmful actions. The OLFC Code states that “adults should be able to read, hear and see what they want”. This appears to be a strong affirmation of freedom of expression but qualifications follow that mandate taking into account generally accepted community standards.

AUSTRALIA’S REASONABLE ADULTS

Who exercises the role of the reasonable adult and upholder of community standards regarding Internet content in Australia and how is this exercised? First, are the legislators who plan and prepare the legislation for the parliament. The group with the most impact are the members of the State and Commonwealth Attorney Generals (SCAG). Second, are the members of parliament that reject, amend or pass any legislation. Third, are the bodies given responsibility for administering legislation. Principally this is the ACMA and the OLFC. They claim that they consult with members of the public, community groups and organisations, including contributors to research.² Recently it has been suggested that the ISPs should be compelled to exercise the role of “Internet cop”. Finally, are the parents or guardians of minors who act as reasonable adults to protect them from Internet content that “is unsuitable for minors”.

The legislators of the relevant acts for the nine Australian jurisdictions rely largely on the various Classification Acts listed as Appendix A. The identification of what Internet content is “prohibited” or “potentially prohibited” at the federal level or is offensive or objectionable at the State or Territory level is dependent on the classification system set out in the Acts. The legislators mandated the system already operative for films as being applicable for the Internet. Presumably they believed that such a system was based on generally accepted community standards.

The legislation for the regulation of pornographic Internet content differs between the States and Territories. The States and Territories have constitutional authority to regulate the authors and consumers on Internet content. Does this signify different community standards for the jurisdictions throughout the Commonwealth of Australia? Probably not as uniform legislation was agreed to at the 1997 SCAG meeting. However, this has yet to be realised.

When a Bill is brought to a Parliament it can be passed, amended or lost. Do Parliamentarians act as “reasonable adults” and are cognisant of Australian or Victorian or Tasmanian “community standards”? The cynic may claim that if the Bill is brought to a Parliament by the Government party all or most government party members will vote for it out of solidarity. All government members voted for the Online Services Bill, for instance, and at best we might suggest they generally believed it reflected community standards. A few expressed the view that more restrictive legislation was required than was passed. Similar experiences occurred with State and Territory jurisdictions.

¹ Both sides claim the research supports their view. The author is of the view that research does not support a direct causal link between pornography and (undesirable) actions. See Wilson and Nugent (1987) and Hargrave and Livingstone (2006) that have analysed the studies.

² Refer to the relevant OLFC URL http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_Research

During the hearings and debates of the Online Services Bill³ the opposition parliamentarians opposed the Bill largely because it was argued that it was not needed and would be ineffective. It was not needed because any activities illegally offline was also illegal if online. It would be ineffective because it could only legislate effectively for onshore content but as over 90% was generated offshore it was beyond the Commonwealth Governments jurisdiction. A cynic may claim that the main opposition party would oppose the Bill or wish to have it substantially amended to be troublesome to the Government. At best we could argue that opposition members held these views because they did not believe it reflected community standards. Insofar as they did at the time of passing the Bill the Federal Labour Party now has a stance little different from the Conservative Coalition on this matter. Indeed in regard to protection of minors it favours more aggressive regulation with mandatory blocking of prohibited (and potentially prohibited) content to households, schools and other public Internet points by the Internet Service Provider. Adults could opt out of the clean feed.

Over time no discernible policy differences exist within a particular State or Territory jurisdiction by the two major parties in regards to classification of pornographic Internet content. As has been noted previously differences do exist between the jurisdictions. This may be confirmation that community standards in Victoria may differ from New South Wales, for instance, as it is reflected in the different legislative requirements.

Under Federal legislation when a complaint is made to the ACMA about pornographic Internet content that is hosted onshore it is classified. The ACMA is bound under federal law to use the established classification system, in this case the one relevant films. The ACMA exercises its role as a reasonable adult in upholding the community standards within the constraints of Online Services and the Classification Acts. If the content is X or RC then it will issue a take down notice to the relevant ISP. If it is classified R but not subject to a ACMA approved verification system a take down notice will be issued.

Where the content has not been classified the ACMA is empowered to “guess” what it might be. The Online Services Act talks of “substantial likelihood”. Similar guessing is required for pornographic content hosted offshore which accounts for over 90% of the total. The ACMA notifies the filter/blocking software makers so they may add such sites to their blacklists. However, in recognition that it is difficult to regulate offshore hosted content, the regime does not include R content even if access to the content is not restricted.

At law minors cannot act as reasonable adults so it is their parents or guardians that act for them. Classified content can provide useful advice to parents in making decisions about Internet content, and other educational and resource information provided by Government cannot also assist. All jurisdictions have as a primary objective the protection of minors from content that may prove harmful so advice, education and provision of filters can be directed to that objective. However, the legislation in its desire to protect minors can deny parental decisions and can also infringe the freedom of expression of adults.

THE CODE AND COMMUNITY STANDARDS

What are some of the major challenges to the efficacy of the current arrangements? They are:

- The Code and Community Standards
- Transparency of Take Down Decisions
- Different State/ Territory Jurisdictional Responses
- Foreign Value Systems
- Impotence of the Federal Regulatory Framework
- Parental Responsibility and the State

Legislation to censor pornography is usually justified by the claim that it is a response to a major concern expressed by the community about it and that there was a need to regulate it online in the same way as offline. This was the case for the Online Services Act for instance. Three observations may be made.

³ Examples for the Commonwealth and the State of Victoria are listed in the References and can be accessed from <http://www.aph.gov.au/hansard/index.htm> and <http://tex.parliament.vic.gov.au/bin/texhtml?form=VicHansard.adv> respectively.

First, no comprehensive study has been undertaken on community attitudes to Internet pornography in Australia. The OLFC claim that Board decisions do reflect community standards but studies are conducted based on the mandated Classification System which is given.⁴ What data exists, for instance Overington (2007), suggest that Internet pornography is not a major concern if this relates to nudity and sexual acts including “real” sex. Overwhelming there is concern for child pornography and to a lesser extent violence. Indeed the refusal of the Coalition to legislate to rename X content (which lacks violence) to Non Violent Erotica (NVE) and ease restrictions would further support the view that there is probably a disconnect between the legislators and community standards⁵.

Second, in the case of the Online Services Act, Internet content is treated as if it were a film. It is legitimate to ask why legislation to regulate Internet content could not be designed for the Internet and not use the classification for completely different media. Certainly the restrictions for a film are more stringent than for other offline media like publications. When Internet content is identical to an article published in an offline magazine or book, the online and offline copies are classified under different Classification Guidelines. An article may be legal offline under the Publications Guidelines, but illegal online when classified under the Film Guidelines.

Third, no classification system can ever be value free. This brings us to the nub of this paper. Censorship in Australia has a long history and we would assert that legislation always lags behind community standards. This is assuming we can define what these are. This is more so with the relatively new sets of technologies we refer to as the Internet. A flawed understanding of the Internet by the legislators has bequeathed many anomalies and absurdities in the legislation. The main point is that the term “community standards” is a misnomer. At best it stands for what most Australians agree should be tolerated. What the majority agree is tolerable may not be reasonable to me if I am of the minority view the adults should be free to access in the privacy of their own home X (or NVE) content currently “prohibited content”. Again, if I am of the minority view that adults should be free to access consensual “demeaning” content this will probably be classified as “prohibited content” also. Such an attitude may not even be a minority view. When the legislators talk of balancing personal opinion with community standards it suggests a “tyranny of the majority” with no “protection” for minorities.

With regard to films, Community Assessment Panels have been appointed to independently assess classification decisions made by the OLFC Board. The OLFC reported (OLFC 2005b) that these panels were more lenient than the Board. More conservative parliamentarians have had a view that Board members are too lenient. Prime Minister Howard, for example, rejected the entire list of candidates for the Board in 1999 exclaiming he wanted “ordinary Australians” (Marr (1999). Presumably these “ordinary Australians” are the people you meet at the footy match or the neighbourhood BBQ. He identifies the reasonable adult with the ordinary Australian which is asserted is as equally hypothetical as the “reasonable adult”.

This extraordinary statement was probably offensive to those “non ordinary Australians” nominated for the Board and is probably evidence that the Prime Minister failed the test of a reasonable adult because he lacked the ability to balance personal opinion with generally accepted community standards.

TRANSPARENCY OF TAKE DOWN DECISIONS

The ACMA acting as a “reasonable adult” in classifying pornographic Internet content lacks transparency as it refuses to give specific reasons for its decisions. This compares unfavourably with films for instance. Ironically it is the film Guidelines that are legislatively mandated to be used by the Classification Boards and ACMA throughout the Commonwealth.

Early in the operation of the Federal Regulatory Framework the Electronic Frontiers Australia (EFA) wished to review the operational effectiveness of it. The (EFA 2000) requested information from the Australian Broadcasting Authority (ABA), the precursor to the ACMA, about the reasons for classification decisions about Internet content. The ABA refused and the EFA made a request under Freedom of Information (FOI). When the information was eventually released most of the information sought was “blackened out”. The ABA justified this on the grounds that the Internet is different from other

⁴ These studies are found at http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_Research

⁵ See for example in the References the Committee Hansard 23 March 2000.

media and making child pornography URLs public may jeopardize policing and legal processes. Subsequently the Administrative Appeals Tribunal ruled against the EFA and later the FOI Act was amended in favour of the ACMA.

This lack of transparency does not allow any independent organisation or the community at large to confirm decisions made by the ACMA are in accord with commonly accepted community standards. Again, it prevents, and this might be the intention, the ability to make a judgement about the effectiveness of the federal regulatory framework. It also undermines the arguments of those who justified legislation to censor Internet content on the grounds that they were ensuring that the same material online is treated in the same way as offline.

IMPOTENCE OF THE FEDERAL REGULATORY FRAMEWORK

Concern by the Federal Government about Internet content probably dates about 1994 when the Department of Communications and the Arts produced a Report on the Regulation of Computer Bulletin Board Systems. At the December 1997 meeting of SCAG it was announced that jurisdictional differences had been solved and new uniform laws were to be passed by all parliaments. The new laws were to make ISPs responsible for Internet content, that is, they would act as reasonable adults and upholder of community standards. An early Online Services Bill had the ISPs responsible under threat of substantial fines to block X material from overseas sites. Recall this is non violent sexually explicit material.

The Coalition Government was finally persuaded that the ISPs should not be compelled to play "internet cops" and that it was a costly and technically difficult exercise. Currently, ISPs are said to comply with the legislation if they provide subscribers with a filter. Indeed while ISPs are notified of prohibited or potentially prohibited content hosted offshore they are not required to block it. However, the ACMA does notify filter vendors that the material must be added to their black list. As we have observed users do not have to have a filter installed.

The Federal Regulatory Framework is largely impotent in terms of its stated purpose. Prohibited and potentially prohibited material hosted onshore can be regulated to some degree. However, such material hosted offshore, and that is over 90% of all content, is not capable of regulation. However, this is not necessarily the case with the States and Territories. They have the power to prosecute "offensive" or "objectionable" content. Prosecution is invariably about child pornography and the critics argue that this was a criminal offence prior to the Internet under the various Crime Acts. No new legislation was required to combat child pornography.

DIFFERENT STATE/TERRITORY LEGISLATURE RESPONSES

Do we believe that community standards differ between the various States and Territories? Is there a Victorian community standard and does this differ from Queensland for instance? If so the legislative responses of the States and Territories towards regulation of Internet content should reflect these differences.

It appears that community standards in Victorian and South Australian demand more restrictive legislation than the other jurisdictions. Both criminalise the making available of content classified as unsuitable for children online even if it is only made available for adult use. In any criminal proceeding the onus of proof is reversed. The accused must prove that the content was for adult purposes and, that all reasonable attempts had been made to protect minors from accessing it. The Western Australian legislation is less restrictive than Victoria and South Australia but makes possession of any content classified RC a criminal offence. The other jurisdictions make only possession of child pornography, a sub set of RC content, a criminal offence.

At the SCAG meeting of 1996 uniform legislation was proposed for the States and Territories to complement the proposed Federal legislation. They are yet to agree to its implementation. One factor at work may be a desire to have legislation that reflects different community standards between the jurisdictions. The Australian Capital Territory (ACT) has relatively liberal laws regarding X rated material (video). It can be legally produced and consumed in the ACT and distributed within it and to other jurisdictions that allow it. ACT acceptance of uniform legislation would make these activities illegal. By contrast the Western Australia legislation explicitly refers to the Internet and it has seen fit

to give police wide powers to search the premises of an ISP and access documents without the need for a warrant. This is not (yet) permitted under the legislation of other jurisdictions. Currently an action on the Internet may be criminal in one State but not in another. X or R Internet content is treated differently between the jurisdictions. Penalties for infringements regarding the consumption and/ or production of Internet pornography also vary between the jurisdictions. Currently, the Commonwealth Government is amending the NT Act to proscribe stronger penalties for the possession and supplying of pornography in areas covered by the emergency response or proscribed areas (indigenous settlements).

One of the virtues of a Federation is supposedly the beneficial balance between the central entity and the other entities that agree to federate. The central entity has responsibility for matters of federal (national) importance like defence. The other entities retain responsibility for those matters important to their particular community (or values or standards) like tourism or transport. However, the history of the Australian federation is that of Federal government dominance of both revenue and expenditure. The trend towards centralisation has been unrelenting and does not appear to be abating. To return to the issue at hand we suggest this argument makes little sense when dealing with the Internet as it is a global medium. This also presents a challenge at the national (central) level and to this we now turn.

FOREIGN VALUE SYSTEMS

The Internet is a global medium and as we have stated before over 90% of pornography comes from overseas, mainly American. National governments worry that their community standards are compromised by citizens accessing and being influenced by foreign content. This applies not only to pornography but other types of content that are viewed as “undesirable” and often made illegal. In closed societies like China and Saudi Arabia the State attempts to censor all types of undesirable content most of it foreign. This requires considerable resources including an army of censors.

In more open societies, like Australia, there is a reluctance to censor to such a degree. However the global trend among all countries is to increasingly censor the Internet. Pornography has long headed the list but now terrorism, supremacist sites and other content are included. National governments are now collaborating together to increase the effectiveness of Internet censorship. There is a tendency for groups like the European Union for instance (CETS 2001), to take all Internet crimes of the member countries and make them applicable to all. Similarly, they apply the most restrictive regulatory framework of the group on all members. Taken to its extreme we might all one day be forced to adopt the value system or community standards of the Saudis. The readiness, driven in the pursuit of profits, for global companies like Yahoo and Google to “collaborate” with dictatorships and theocracies perpetrating serious human rights violations is also a worrying trend. Australia cannot be immune to these trends.

PARENTAL RESPONSIBILITY AND THE STATE

Governments throughout the Commonwealth all agree that parents should decide what their minors are permitted to access on the Internet. Governments claim that they are there to support parents in this role. They do this mainly through the consumer advice provided by the classification categories, education through bodies like NetAlert and the requirement that an approved filter be made available by the ISP if the household requests it.

However, many in the parliaments believe the role of the State should be greater than providing advice to, and education for, parents. During the hearings and debates of the various Federal and State legislation some respondents expressed concern that many parents lack technical knowledge to properly supervise their children's access to the Internet. They painted a picture of a “technical savvy” child only too ready to successfully deceive its parents. They argued the State needs to counter these deceiving children. Many respondents also were worried about irresponsible parents who did not properly supervise their children's access and argued the need for the State to counter this. The State should protect children from their irresponsible parents. Of course there is precedent for this in other areas. During the hearings and debates similar concerns were expressed about librarians. It was argued that their dedication to free expression could endanger children or they were simply too busy to properly supervise minor's access to Internet content in the library. Mandatory ISP filtering as proposed by the Federal Labour Party appears to usurp parental responsibility and impose a standard foreign to many households.

What limited data we have, and this comes from an ACMA Report (ACMA 2005-06) suggests that most parents of children aged 8-13 do not have Internet filters installed. Is this confirmation that parents are not technical savvy and/ or irresponsible? The limited evidence suggests the contrary. Fifty percent of parents do not install filters because they trust their child and only 5% were unsure how to install the filter. Indeed the same Report stated that 92% of parents reported that they were involved in their child's Internet use in some way and 67% reported supervising their child's Internet use by watching their activity to some degree.

CONCLUSION

This paper examines two questions concerning the exercise of the reasonable adult test in relation to Internet content illustrated with reference to pornography. First, who exercises the role of the reasonable adult and upholder of community standards and how is this exercised? Those identified were the legislators and parliamentarians of the Commonwealths nine jurisdictions. They have largely indicated what they believe community standards to be as they probably consider themselves "ordinary" Australians. Obviously the legislation constrains the choices bodies like the Classification Board and the ACMA make in regards to specific pornographic Internet content. The legislation also constrains parental choices about minors their use of the Internet for which they have responsibility.

Second, what are some of the major challenges to the efficacy of the current arrangements? There is probably a disconnect between actual community standards and what legislators and parliamentarians believe they are. Confidence in the efficacy of the federal regulator framework is seriously impaired by the lack of transparency with ACMA take down decisions. Indeed the current framework appears to be impotent as it lacks jurisdictional control over 90% of "prohibited" or "potentially prohibited" content. Most State and Territory governments have failed to pass the uniform model legislated agreed at SCAG that would complement the Federal legislation. The global nature of the Internet and global efforts to heavily censor the Internet will impact negatively on Australian values and norms. There is a concern that government in Australia usurps parental responsibility for minors in this area even if done for the best intentions.

REFERENCES

Australian Government (2006). *ACMA Communications Report 2005-06*. Australian Communications and Media Authority.

Commonwealth of Australia (2000). *Legal and Constitutional committee: Reference: Classification (Publications, Films and Computer Games) Amendment Bill (No. 2) 1999*. Thursday 23 march. Senate Hansard.

Commonwealth of Australia (1999). *Senate Select committee on Information Technologies. Reference Broadcasting Services Amendment (Online Services) Bill 1999*, Senate Official Committee Hansard.

Commonwealth of Australia (1999). *Second Reading Broadcasting Amendment Services (Online Services) Bill 1999*, Senate Hansard.

Commonwealth of Australia (1999). *Second Reading Broadcasting Amendment Services (Online Services) Bill 1999*, House Hansard.

Council of Europe (2001). *Convention on Cybercrime*. ETS No. 185. Budapest.

Electronic Frontiers Australia (2000). FOI Request on ABA Report on Documents Released/ Denied. http://www.efa.org.au/FOI/foi_aba_2000.htm date accessed 27 November 2007.

Hargrave A and Livingstone S (2006). *Harm and Offence in Media Content: A Review of the Evidence*. Intellect books, UK.

Marr David (1999). *Cabinet X-Rates New Censor List*, Sydney Morning Herald. May 8.

Office of Film and Literature Classification (2005a). *Guidelines for the Classification of Films and Computer Games*.

Office of Film and Literature Classification (2005b). *Community Assessment Panels*. urbis keys young, February.

Overington Caroline (2007). *Be Adult, Porn Industry Pleads*. The Australian, February 28.

Parliament of Victoria Hansard (1995). *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995*. Second Reading, Assembly, 15 November p 1179 and 16 November p 1290.

Parliament of Victoria Hansard (1995). *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995*. Second Reading, Council, 1 November p 405 and 14 November p 486.

Wilson P and Nugent S (1987). *Sexually Explicit and Violent Media Material: Research and Policy*. Australian Institute of Criminology, Canberra, Vol.1, No. 7.

Appendix A Relevant Current Legislation

Commonwealth

Classification (Publications, Films and Computer Games) Act 1995
Broadcasting Services Amendment (Online Services) Act 1999

Australian Capital Territory

Classification (Publications, Films and Computer Games) (Enforcement) Act 1995

New South Wales

NSW Classification (Publications, Films and Computer Games) Enforcement Act 1995

Northern Territory

Classification of Publication, Films and Computer Games Act

Queensland

Classification of Computer Games and Images Act 1995
Classification of Films Act 1991
Classification of Publications Act 1991

South Australia

Classification (Publications, Films and Computer Games) Act

Tasmania

Classification (Publications, Films and Computer Games) Enforcement Act 1995

Victoria

Classification (Publications, Films and Computer Games) (Enforcement) Act 1995

Western Australia

The Western Australia Censorship Act
Classification (Publications, Films and Computer Games) Enforcement Act 1996

Copyright

Geoffrey A Sandy © 2008 The author assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

The Ethics of Compulsory Open Source

Judith Thomson,

Murdoch Business School,

Murdoch University,

Murdoch, W.A.

Email: j.thomson@murdoch.edu.au

Abstract

Open Source is increasingly attracting attention as Microsoft has formed connections with computer companies based on Open Source philosophies. But among its adherents are those who insist that the source codes of all computer programs must be freely available to everyone, and who decry the use of intellectual property laws to protect computer programs at all. This paper seeks to examine the semantic, ethical and practical bases of their arguments and to show that they are based on some fundamental and vitiating ambiguities. Furthermore, taken to their logical extreme, such contentions could have serious economic implications for the way Western society operates. Voluntary Open Source may be entirely admirable from ethical and practical perspectives, but Compulsory Open Source has little to recommend it.

Keywords – computer software, compulsory open source, ethics, ‘free’ meaning costless, ‘free’ meaning unfettered, information content of computer programs, ‘primary’ information, ‘secondary’ information, Utilitarianism, voluntary open source.

INTRODUCTION

In mid-October 2007 Microsoft announced a new level of co-operation with Open Source initiatives. This is almost certain to spark debate about Compulsory Open Source in some quarters of the computing world, which in turn raises some very interesting ethical questions. Advocates of Compulsory Open Source are often quite passionate and have a number of ethical arguments to support their views – it is the sustainability of these that is now under consideration. Should source code really be free, and if so why?

The benefits of Open Source are easy enough to see – really cheap software which is continually being upgraded and made more effective. Who would not want this? What arguments could possibly be mounted against it, except, of course, by companies who shall be nameless but who have vested interests in keeping software prices high? But unfortunately the implications of Compulsory Open Source go much deeper, to the point of shaking the foundations of Western society.

Ethical arguments in favour of Compulsory Open Source: One contention often advanced in favour of Compulsory Open Source (Moglen 2003; Stallman 2002) is that there is an ethical right for all people to share computer programs because -

1. They consist of information, and information should be free for all, and
2. There is no justification for the imposition of costs here since the marginal cost of duplicating each computer program is zero i.e. free.

Let us examine each of these statements.

1 (a) *Do computer programs consist of information, and if so, in what sense?* In ordinary speech “information” is knowledge relating to some fact(s). These facts could be facts that – e.g. that Everest is the highest mountain in the world, that Freud held certain beliefs about the genesis of human behaviour. Let us call these facts that X is the case “primary information”. By itself primary information may be interesting but is not immediately useful. It is not protected by either copyright or patent law, and so it is already open for all mankind to the extent that the discoverers of this information choose to make it public.

Alternatively information could consist in statements of how to do something - facts that have been adapted/ harnessed to be useful, e.g. how to climb Mt Everest, how to combine hydrogen and oxygen to make water, how to carry out Freudian psychoanalysis. Let us call these how to facts “secondary information” because “how to” facts are predicated on a basis of “facts that” certain situations exist, e.g. to make water one combines oxygen and hydrogen in a certain way because water consists of one molecule of oxygen to two molecules of hydrogen.

Is secondary information protected by law? Yes, if it can meet certain criteria. Primary facts that have been harnessed in novel, ingenious and practical ways can be protected for 20 years from the priority date of the patent application, whilst tricks of trade – e.g. secrets of bookbinding craft, of engineering processes, of marketing techniques – may be protected by confidentiality law or trade secrets if they too meet requisite criteria. In each case the law is protecting the investment of labour, skill or ingenuity and time which has resulted in the harnessing of raw data to produce a commercially useful result. And this is entirely consistent with the view underpinning the kind of society in which we live, that a person is entitled to profit from the sale of his skill or labour and from the products that result from the investment thereof.

Having noted the difference between primary and secondary information, and having clarified the rationale for protecting the latter but not the former, it remains to stress the need to distinguish the *means* of conveying information in either form from the information itself. Copyright protects the form of expression of an idea, not the content expressed. The raw facts in an article on Mt Everest are available for all to use as far as concerns copyright law. What cannot be done - at least during the life of the author of the article plus the 70 year statutory period - is to reproduce the form of words by which this information is conveyed. Similarly, where patent applications embody primary information, this can be utilised by all. Protection extends only to the harnessing of this raw data in some new, non-obvious and useful way, and then only for a limited period – usually 20 years.

We can now consider the extent to which computer programs consist of information, and of what sort. Programs are written initially in source code, complete with comments, and then transcribed into object code without the comments. Consequently object code consists of a series of commands which are directed to the computer and which make the computer achieve certain states. Clearly computer programs such as the Encyclopaedia Britannica are heavily freighted with primary information, and the words in which this is conveyed are protected by copyright, though the raw information itself is not, and is available for use by all consulting the program. Games and tools such as Photoshop and Word may be relatively free of primary information, depending on their didactic nature, but once again such primary information as they contain is available to all comers.

But what about the codes in which the programs are expressed? As they are deemed by section 10 of the Australian *Copyright Act 1968* to be literary works, they have traditionally fallen under copyright protection insofar as concerns the coded statements which comprise them. Do they consist of information? Indeed they do. Source code contains considerable secondary or ‘how-to’ information in the form of explanatory comments, and will almost certainly be rich in secondary tricks-of-the-trade information relating to ways of achieving certain ends to make the program perform satisfactorily. It is this secondary information that Compulsory Open Sourcers crave – since any primary information contained in programs is already freely available to them.

(b) *Granted that computer programs contain information, what are the arguments for information being free?* The right to freedom of information is a common contention of compulsory Open Source protagonists, but is usually based on an illicit modulation between primary and secondary information and between two different uses of the word ‘free’. On the one hand ‘free’ can mean ‘not subject to constraints on availability’, whereas on the other it means ‘not costing anything’. Freedom in the first sense will not necessarily entail gratuitousness in the second.

(i) *Free in the sense of accessible by all* : Is there some ethical imperative that primary information should be free in the sense of being unconstrained by laws regulating its availability? Certainly there is a strong case for primary information of public importance and interest being easily accessible. Raw scientific, historical or cultural data should be available to all, and to a large extent this has been the case even where intellectual property such as patents have been granted over inventions utilising the information. The primary information is available to all without constraints through the patent specifications, although patented processes (secondary information utilising the primary information) may not be harnessed without financial cost in the form of royalties to the inventor.

There are good reasons in western society for not requiring *secondary* information to be freely available in either sense. Investing time and gaining skills are typically the sorts of sacrifices thought to be compensable by wages or receipt of a purchase price for the resultant product or service, and any change to this would result in the foundations of our society radically altering. It may be that a capitalist society has serious problems, but it is the one in which most of us have elected to live and should not be changed without serious consideration.

(ii) *Free in the sense of costless*: Open Source proponents have been known to jump illegitimately from an argument for free - i.e. unconstrained and accessible – information (often involving a confusion of primary and secondary information) to one for free (i.e. without cost) information. This usually involves a discussion of the marginal cost of reproduction of digitised information. Marginal cost is the cost of producing one extra unit after the initial setup and raw material costs have been absorbed. Typically it is considered when one has set up, for example, a manufacturing business which already supplies widgets to the local market and one is contemplating the financial viability of expanding into a new market, perhaps overseas. Before the marginal cost becomes relevant, one must first cover the costs of creating the original home-market widgets, with all the necessary experimentation, labour costs, expenses of establishing a factory, tooling up, purchasing raw materials and fine-tuning to meet market expectations. Applying this to Open Source arguments, the cost of reproducing a computer program would have to take into account the cost of developing the program in the first place. The fact that the marginal cost of reproducing the one millionth copy of a program is infinitesimal is absolutely no argument for not recouping one's production costs over the first 999,999 copies. And if the first 999,999 customers have to pay to purchase the program, it may lead to considerable disgruntlement when the last paying customer discovers that, had he or she waited a few more hours, he or she would have been the first of the non-paying recipients since the production costs had now been amortised. At the very least, this would make planning an equitable marketing strategy extremely difficult. As a potential purchaser it would seem preferable to have a constant purchase price, even when the marginal cost has sunk to virtually zero – if indeed the program lasts long enough for this to occur. Given the short life of many programs, this is not a foregone conclusion. That some of us feel that we are being severely exploited by some software producers who enjoy almost monopolistic marketing conditions is not an argument for abolishing pricing altogether, but rather for introducing competition and, if necessary, legislating to prevent price gouging.

On the basis of our own foregoing analysis it appears reasonable that -

- **primary information** should be freely available, though perhaps not necessarily financially free since it may have cost the discoverer a considerable amount in terms of time and expensive technology to ascertain the information. Where this is the case, it would not be unreasonable to expect that some sort of payment should be made at least until the cost of discovery of the information has been recovered.
- With respect to **secondary information** there seems to be no serious argument that labour skill and ingenuity should not be compensable, and the expenditure of these same qualities to produce works of literature or art which do not constitute "information" should similarly be rewarded by cash value. Is there an argument that secondary information/ tricks of the trade should be openly accessible? No. It is socially desirable that skills be imparted from one generation to the next, but these skills are often the basis of industries – e.g. winemaking, engineering, china manufacturing) and what is important is the perpetuation of the skills which take time and skill to impart and learn. Undoubtedly the quality of wines throughout the world would rise if all the in-house secrets were learned and placed on the internet, but this is not an argument for so doing. Compulsory acquisition and commercial espionage are both viewed unfavourably by a free society.

Compulsory Open Source arguments sometimes seem to constitute special pleading for those computer program writers who want access to the source code created by others, without establishing any solid grounds why this should be so and without considering the effect of this as a precedent either for those software writers who are of a different persuasion regarding their intellectual property rights, or for the rest of society.

Pragmatic Arguments for involuntary open source: There are two more lines of argument often run in favour of Open Source software both of which deserve to be considered, as one carries weight. The first one can be quickly disposed of, and it takes the form of an argument that exclusionary intellectual property rights are bad because their imposition constitutes a practice involving “the large-scale continuance of unnecessary ignorance”(Moglen 2003 para 7). This ignorance is said to accrue to the benefit of certain vast institutions. This would be essentially immoral if the charge were true. It would also have very important practical implications for society. It is alleged that societies which embrace intellectual property rights teach children “that it is wrong to share information” and that they should accept the need for licensing (Moglen 2003 para 8). Again, the ambiguity in the word ‘information’ is exploited with a conflation of abstract primary information - which should morally be available to all but which is not subject to exclusive intellectual property rights anyway - with the functional implementation thanks to human skill and labour, of ideas which constitutes secondary information. Licensing recognises and protects the value of the skill and labour components, and to teach children to ignore licensing provisions is to teach them to steal other people’s property.

More importantly, as we have already seen, this contention is legally wrong. Patents do not contribute to ignorance, since the consideration for obtaining a patent is that the patentee must teach the best known method of performing the invention - and this information is publicly available to all from date of granting of patent. To the extent that the information contained in the patent specification is primary in nature it can be used immediately and free of cost. To the extent that it is secondary, it cannot be used without payment of royalties, for reasons discussed, for 20 years. Copyright contributes to unnecessary ignorance only to the extent that the relatively small amount by which the royalty fee raises the cost of books; and books (and free lending libraries) are dedicated to the destruction of ignorance. But it seems that the argument is not really concerned with any intellectual property right which does not apply to computer programs. The objection is usually to copyright as it prevents software writers from getting at the source code and scrutinising and utilising the code therein which enables certain special effects to be obtained or special steps to be performed. But as this code and the accompanying comments are products of the writers skill and labour, there seems to be no more reason why other programmers should appropriate these freely than there would be for writers of textbooks to copy each other’s expression rather than understanding the raw information and working out their own novel ways of conveying this.

The second pragmatic argument in favour of Open Source links in to the first one and is essentially Utilitarian. It holds that there are sizable advantages for society if Open Source is the (compulsory) rule since it will provide better quality programs, and programs that - where defective - are fixed much quicker. Moreover, freed from the expense of intellectual property rights enforcement and from administrative costs, programs would be cheaper and more flexible. This is all true, and constitutes a strong reason for welcoming some form of voluntary Open Source. But in all Utilitarian arguments it is necessary always to balance the benefits against the known harms to society – and in this case the manifest harm to western society as we know it, of denying the principle that free persons are entitled to sell their skills and time and the products thereof in free markets completely outweighs the benefits to software writers and users of cheaper, more flexible software. This is especially the case since it is not a choice between software and no software, but a choice between adequate software and better, cheaper software.

The Utilitarian calculus thus suggests that whilst software is subsumed under normal intellectual property rights there is no benefit, and much harm, for society from compulsorily requiring programmers gratuitously to reveal their source code. Unless a case can be made for separating creation of computer code from other currently protected forms of creativity, compulsory Open Source would bring more losses than gains overall. However, as we shall see later, this is not to suggest that the present regime is optimal with respect to computer programs and their protection.

Two further contentions re Compulsory Open Source need to be assessed. The first is that copying intellectual property is different from stealing a physical object, since it does not deprive the creator of

anything he possesses (Stallman 2002). But are material possessions so different from intangible possessions? If I am reading a copy of a current best-seller, or if I am drinking from a mass-produced tea cup and you steal it from me, this is a nuisance. I will either go without or have to buy myself a replacement. In this case I will pay for it using money – which is a means of storing value. And the value it stores has become mine because I exchanged my skill and time to earn it. Thus it could be said that my material possessions are often the physical embodiment of the returns on my investment of labour and skill. By stealing the material object, you have cost me money – which is to say that you have cost me the time and skill which I must reinvest to earn the money to replace the object which you stole.

Similarly, when you make an unauthorised copy of a computer program which I have written, you are effectively stealing the time and skill I have invested in that program and either you are arrogantly assuming that I should work for you for no cost or that I have no right to sell my skills and time to those who will pay for them. Either way, you are stealing the essence of my work – which is also the essence of what is necessary for me to live in a market economy.

The second argument involves an attack on the idea that intellectual property rights stimulate the production of software. This may be countered with the observation that if there is a strong unmet demand for a certain sort of program, programmers will normally respond by filling this gap in the market. Certainly this does not happen at the moment in all areas, but the fact that several large software companies are exerting an unhealthy stranglehold over the free market does not invalidate the argument for intellectual property rights, it simply indicates the need to break a market monopoly situation which would be undesirable in any area, not just with respect to software.

Apart from exploitative pricing by monopolist producers (a flaw in market regulation rather than in the intellectual property law system) a problem with respect to intellectual property rights occurs in the area of purpose-designed software. Most computer users e.g. lawyers, accountants, managers, writers etc., will never write or really need to create their own software, but large corporations and scientific researchers may do so. Many persons in large corporations and in scientific research will not be able to write their own programs, but they may be able to tell a computer programmer what they would like to be able to do. And this is where it is freely admitted that access to source code would save programmers from having to reinvent the wheel and write their own programs from scratch. However the overthrowing of the fundamentals of western society seems to be too high a price to pay to satisfy this need. It is inefficient and regrettable, but it is less bad than the alternative.

Conclusion: Thus it appears that compulsorily requiring the disclosure of source code cannot be justified on either ethical or Utilitarian grounds, as the cost in terms of the overthrowing of democratic society would vastly outweigh the benefits of better computer programs more quickly. This is not to suggest, of course, that voluntary open source sharing is not an excellent idea for those who wish to participate. It is also possible that some *sui generis* form of legislative protection might be devised which would justify treating source code in a way entirely different from other forms of property (and thus avoid setting a precedent for these other forms). What is clear is that whatever the outcome, any disenfranchisement of rights must be on a purely voluntary basis either by small groups of like-minded programmers or by the informed consent of democratic voters.

REFERENCES

Moglen, Eben (2003) *Freeing the Mind: Free Software and the Death of Proprietary Culture* keynote address at the University of Maine Law School's Fourth Annual Technology and Law Conference, Portland, Maine, June 29, 2003, available at <http://emoglen.law.columbia.edu/publications/maine-speech.html> Last accessed 7/1/08.

Stallman Richard (2002) "Why Software Should Not Have Owners" in *Free Software, Free Society: The Selected Essays of Richard M. Stallman*, available at <http://www.gnu.org/philosophy/why-free.html> Last accessed 7/1/08

Copyright

Judith Thomson © 2008 The author assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

Expanding the IT Territory: Creating Space for Ethical IT

Ian Stoodley
Christine Bruce

Faculty of Information Technology
Queensland University of Technology
Brisbane, Australia
Email: i.stoodley@student.qut.edu.au

Abstract

This paper proposes a three dimensional model representing the IT territory, with a view to incorporating ethical professional practice as integral to the discipline. The evolving nature of the IT discipline is mapped along Information-Technology and Developer-User continuums and the ethical nature of the IT profession is mapped along an Inward-Outward continuum. Suggested uses for the model include a reconceptualising of the IT professional space, guidance for ethical formation and support, and inspiration for individual and organisational standards.

Keywords

Professional ethics, Information technology, Conceptual model.

INTRODUCTION

The Information Technology (IT) territory has been historically conceived in a technology-centric way. This has led to an artefact focus, where hardware and software development has predominated as the core business of IT, with only superficial reference to the users and their context. As such, user needs and social factors have been left largely unexplored (Alter, 2003, Finkelstein and Hafner, 2002, Orlikowski and Iacono, 2001). This influences discipline experts' and practitioners' expectations of what is included in the IT field and how they should engage with it, including the way they understand what it means to be ethical in IT professional practice. What is needed is an expanded conceptualisation of IT, which brings the user into focus and integrates ethics into its identity. Such a reconceptualisation may provide the foundation from which to build a radically different IT profession. This paper proposes a reconceptualisation in the form of a *Model of Ethical IT*.

WHAT IS THE MODEL?

The *Model of Ethical IT* serves as a means of visualising the IT space from an ethical standpoint. It is intended to help IT professionals redefine the dimensions of the discipline and assess their role in it. It challenges technology-centric views of the IT discipline, practitioner-centric definitions of professional practice and ego-centric views of ethics by offering a perspective which focuses on information, clients and humanity.

HOW AND WHY WAS THE MODEL DEVELOPED?

A new model provides a foundation on which to build advances in the field. This model is designed to facilitate a re-framing of the IT territory and to consequently change our expectations of it and our behaviour in it.

The model is a confluence and interpretation of IT research literature, previous research by the authors, and interviews from a current project.

A reading of the IT literature and previous research reveal a range of opinion regarding the territory of IT. In the literature such diversity is evident, for example, in Lenox and Woratschek's (2003) observations on the relationship between IS and IT, and Orlikowski and Iacono's (2001) commentary

on conceptions of the IT artefact. Our previous research (Pham et al., 2005, Bruce et al., 2004) disclosed a range of views amongst IT students, academics and practitioners (also Bruce, C., Stoodley, I. and Pham, B. 2007, *Constituting information technology research: The experience of IT research students*. Submitted for publication). The model presented here is an attempt to first represent, then extend this diversity of opinion by incorporating an ethical dimension based on perspectives of ethics as yet unexploited in the IT literature.

The model began with a two-dimensional *Model of Evolving IT* (depicted in the central rectangle labelled 'Traditional IT -> Evolving IT' in Figure 1), which mapped the apparent evolution of the IT space from its traditional technological roots to a more user- and information-centred perspective (Stoodley, I. 2007, *IT professionals' experience of ethics and its implications for IT education* presented at the Doctoral Consortium of the 18th Australasian Conference on Information Systems, accessible through <http://eprints.qut.edu.au/>). While this two-dimensional model successfully identified a breadth of IT professional practice, it failed to adequately account for the ethical aspect. This aspect has been added to the *Model of Evolving IT* as a third dimension, depicted in the two outer rectangles in the *Model of Ethical IT* labelled 'Client' and 'Humanity'. An ethical orientation is evident in the literature, including concerns about a lack of criticism of established beliefs and goals (Kling, 2003), and predictions that a limited vision means a limited future for the discipline (Orlikowski and Iacono, 2001, Denning, 2001b). The ethical aspect is also strongly supported in interviews in the current project, as illustrated later (Stoodley, I. 2006, *IT professionals' experience of ethics and its implications for IT education: Confirmation of candidature* presented at the Queensland University of Technology, accessible through <http://eprints.qut.edu.au/>).

The *Model of Ethical IT* offers a view of the ethical nature of the IT discipline, providing a point of reference for conversations about ethical practice in the discipline and a stimulus for individual or group reflection.

WHAT DOES THE MODEL LOOK LIKE?

This section describes the model and the next section indicates its theoretical basis.

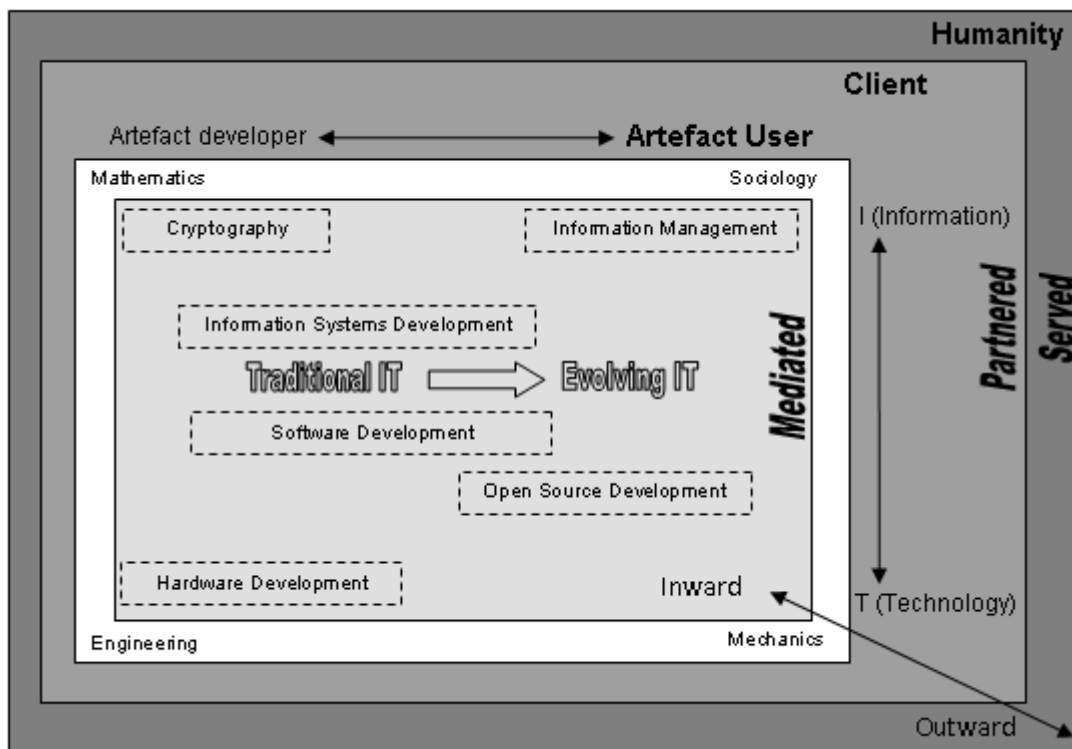


Figure 1. A Model of Ethical IT

The *Model of Ethical IT* (Figure 1) represents *Traditional IT* and its development into *Evolving IT*, these together comprising the presently emerging IT territory. A critical feature of the *Model of Ethical*

IT is the representation of an outward-looking perspective, embracing progressively the *Client* and *Humanity*.

Modelling the IT discipline

The inner rectangle of the model depicts evolving IT. *Traditional IT* (the left-hand side of the inner rectangle) represents technological development with little reference to application. This is artefact- and data-oriented, and concerned with efficiency and overcoming barriers to technological advances, as presented by the technology itself. *Evolving IT* (the right-hand side of the inner rectangle) mediates this technological development to people. It is user- and information-oriented, and concerned with meeting needs defined outside the technological community. The combined *Traditional* and *Evolving IT* represent the trend of IT, with both artefact development and mediating roles included as part of IT. Mediation is understood here to include enabling users, but also acting as an intermediary between the user and the artefact.

In the current project, a user orientation formed the foundation to an ethical interaction:

I think a lot of the problem with IT professionals' ethics are that they assume a godlike complex in some ways... where they say, "We know what's good for you... so, this is the answer." Whereas, the reality is IT are enablers... and so when someone comes to them with issues or problems... they should be looking at facilitating rather than necessarily saying, "I know this is what's good for you."... (Interview 24)

Specific activities are suggested inside the IT rectangle (for example, Hardware Development and Cryptography), in an attempt to concretely illustrate the space.

The reference disciplines of Mathematics, Engineering, Sociology and Mechanics, in the border surrounding the inner rectangle, suggest the outer limits of the IT space. These remain distinct from the IT discipline, though having an influence on it.

Modelling the ethical aspects of IT

The outer rectangles of the *Model of Ethical IT* depict a further development of the ethical aspect of IT, portrayed as client-based and humanitarian orientations. This third dimension, an *Inward-Outward* continuum, represents increasing acceptance of responsibility for others. Along this third dimension the client layer represents a focus away from the IT practitioner's world, towards partnering with clients. This constitutes a fundamental conceptual step on the part of the practitioner from technician to professional, placing the client and their needs in the centre of the practitioner's conception of their practice.

In the current project, partnering with clients established an ethical relationship:

If a customer is getting to the point where they're blindly implementing something... and we know there will be problems because of our knowledge that we couldn't have known about if we had just been... a cold call, if you like... then I think... we need to say, "Look, you can do this but there are things that you need to know about"... knowing that they'd appreciate our view on something because they see us as a trusted adviser as opposed to just someone that's supplying a piece of tin... (Interview 12)

The Humanity layer represents a further step outward, away from the professional's world, to where the professional sets aside their own agenda in the service of Humanity. ('Humanity' here refers to people who do not necessarily relate directly to the professional but who would benefit from the professional's services.) This constitutes a conceptual step on the part of the practitioner to being a professional leader, or master, placing humanity's needs in the centre of the practitioner's conception of their practice.

In the current project, a focus on Humanity determined the conduct of ethical business:

... part of my attraction to it is that... it turns the IT industry back into a services-based industry, where you get paid for the time and effort you put in and not for the results of that time and effort that then you can use over and over again to make money at no effort to yourself... I don't think that that model takes into account the disparity between the rich and the poor in our world today, I mean when three billion people apparently go to bed hungry each night I don't think large corporates have any excuse

for trying to wheedle the last cent out of you and me. I think that money can be put to far better uses. (Interview 9)

The outer layers in this model influence professional practice at the inner layers. For example, the Humanity layer helps a professional answer the question: "What if a client asks you to exploit other people on their behalf?" The outer layer also challenges the professional to include in their portfolio activities that offer no reimbursement but which help meet the needs of the underprivileged.

WHAT ARE THE MODEL'S THEORETICAL UNDERPINNINGS?

This model, then, is structured on an understanding of ethical IT as defined three dimensionally by an Information-Technology Continuum, a Developer-User Continuum and an Inward-Outward Continuum. The IT discipline is understood to be evolving, while maintaining its distinctiveness from certain reference disciplines which lie at its periphery and help define its limits.

The Information-Technology Continuum

Previous empirical research (Pham et al., 2005, Bruce et al., 2004) has revealed IT researchers conceptualising their research field in terms of information and technology, with some emphasising the development of technological artefacts and others emphasising the use of information. In the wider literature, these perspectives are represented by Orlikowski and Iacono (2001) who reviewed IS articles' treatment of the IT artefact, finding some researchers focus on information technology as an artefact while others focus on the information manipulation which the artefact enables. Similarly, Gorgone (2001) acknowledges artefact developers but says IT includes "knowledge workers" (p.11). In 2002 the IT Deans Group of the Computing Research Association of North America proposed "a new IT discipline with a new research agenda" which included study of information... "how it is acquired, organized, communicated, managed and used by people and organizations, and how IT changes those processes, sometimes in fundamental ways" (Finkelstein and Hafner, 2002). Thus, the relationship between information and technology is fundamental to the IT discipline.

The Developer-User Continuum

Previous empirical research (Pham et al., 2005, Bruce et al., 2004) has also revealed IT researchers drawing a clear distinction between IT artefact developers and IT artefact users, with some researchers privileging developers as constituting the 'core' of IT. The central role of the artefact as a defining element of IT is evidenced in a Computing Research Association categorization of IT jobs, which defines each one in terms of its relation to the IT artefact (Freeman and Aspray, 1999). A distinction between the developer and the user is also made in the literature (Armitage and Karshmer, 2003), though some acknowledge the difficulty in doing so and question where the line between them should be drawn (Kaarst-Brown and Guzman, 2005). Denning and Dunham (2001) argue for the need to move from technology-centred to customer-centred development, claiming elsewhere (2003) that the customer is currently not present in developers' awareness. Thus, the relationship between artefact developers and artefact users is also fundamental to the IT discipline.

The Evolving IT Concept

Many writers expand the definition of IT beyond artefact development. Denning, commenting on the scope of Computer Science, observes, "Today, programming is neither the dominant practice nor the defining practice" (2004, p.18). Thus, IT definitions include intensive users (Denning, 2001a), and services such as consulting and support (Iansiti and Richards, 2006).

Traditionally we think of the IT professional as computer scientists (CS), computer engineers (CE), information systems analysts (IS), software engineers (SE), and computer programmers. The scope of the IT worker is much broader than that. It includes consultants, knowledge workers that use technology, and the many other professions that work... to identify, analyze, propose, implement, improve, maintain, and use information technology-based solutions. (Gorgone, 2001, p.11)

Others argue that the IT artefact needs to be "put in its rightful place" and viewed as part of wider "IT-reliant work systems" which include the user's perspective (Alter, 2003, p.370). Thus, we see IT evolving over time, broadening from its technological roots.

The Periphery

Outside the IT discipline lie reference disciplines which contribute to IT. For example, engineering and mathematics are identified by Denning, et al. (1989) and McGuffee (2000) as disciplines which have

contributed to the development of IT, while remaining distinct from it. These help define the outer limits of the IT territory.

The Inward-Outward Continuum

Some IT literature suggests that a change from a primarily technical perspective of IT requires inclusion in the IT universe of “the impact of technology on society” (Finkelstein and Hafner, 2002, p.2) and the “people that define a social context” (Orlikowski and Iacono, 2001, p.122). The following supports and enlarges such inclusions, based on an understanding of ethics, professional ethics and the current IT environment.

With respect to ethics, Emmanuel Levinas defines ethics in terms of responsibility to the Other (meaning other people) (Critchley, 2002). This responsibility cannot be avoided, as our encounter with the Other calls such responsibility forth from us and engages us as ethical agents. Our place in that relation is not one of an equal but of a servant, obligated by our responsibility towards the Other. Such obligation is not so much conscious, as a responsiveness to the Other. Seen thus, ethics calls egoism into question and moral consciousness is seen not as “an experience of values, but an access to exterior being” (Critchley, 2002, p.150). Such a view describes ethics in terms of our relation to others, rather than as a list of rules. Critchley (2002) suggests that this lays the kind of foundation upon which ethical rules can and must be built.

With respect to professional ethics, Darryl Koehn (1994) argues that the only defensible ground for professional ethics, which serves as a legitimate reason for clients to trust the professional, is the professional's promise to provide certain services on the client's behalf. This promise is made implicitly, if not explicitly, when the professional accepts the role of a professional. It underpins any formal contract that may be entered into and guides the application of the professional's expert knowledge. It alone provides the basis upon which a client may trust a professional to conduct themselves in that client's best interests.

With respect to the current IT environment, promise-keeping is identified by Denning and Durham (2001) as a new “third wave” (or Information Age) characteristic of the relationship between the IT professional and their customers. In this new, post-industrial era, the customer is the driving force in business, not the producer. Professionals distinguish themselves by establishing value-generating relationships, with ‘value’ defined by the customer. The role of the professional is to satisfy the customer.

In other words, Levinas illuminates a basis on which to build ethical rules, Koehn asserts the ground for ethics in the professions, and Denning and Durham observe the reality of professional practice in the current Information Age. Their focus on the Other, the client and the customer indicate the necessity for the professional to adopt an other-centred attitude. Such an attitude is imperative, for professional practice to claim to be ethical. This suggests the continuum of inward looking-to-outward looking which defines the ethical axis in our model.

HOW CAN THE MODEL BE USED?

The *Model of Ethical IT* primarily serves as a conceptual tool, to represent the relationships between people, artefacts and activities in the IT space. Such a conceptual tool could be used on an individual, group, organisational, professional or discipline level.

The model may be used:

- to reconceptualise the IT professional space;
- to plan future directions;
- to provide guidance of ethical formation and support;
- to define the scope of the IT profession's ethical responsibility;
- to provide inspiration for individual and organisational guidelines;
- to set standards of conduct and aspiration; and
- to aid communication between stakeholders.

It may be used in a strategic sense, to orient activities towards certain goals or outcomes, or it may be used in an operational sense, to evaluate specific actions.

The model may be used to present a vision to practitioners, of who they may become. Interaction with the model could serve to modify their understanding of IT professional practice and effect a behavioural change, flowing from a conceptual shift.

The central role of conceptualisations in determining our expectations of IT and the way we interact with IT indicate the key role they play in its deployment, and affirm the potential power of such a model.

FUTURE RESEARCH

A greater understanding is needed of how the model may be applied, as suggested in the previous section. As such, its use in establishing and implementing educational programs, its use in evaluating and adjusting business practices, and its use in creating and promoting professional codes are all areas in need of further investigation. Currently, empirical research into IT practitioners' experience of ethics is being analysed, which should indicate in more detail the existing degree of alignment between practitioners' views and the model proposed here. The model should also be tested against further empirical evidence of IT professionals' experience of ethical practice.

CONCLUSION

The *Model of Ethical IT* presents an expansion of the IT territory to focus on information and clients, and to turn ever outwards towards those it may serve.

This attitude alone, of concern beyond the artefact, provides sufficient reason for IT professionals' clients to trust them. Thus, central to the model is a charter to partner clients and serve humanity. For IT professionals these are not optional extras, but must be integral to their practice if they are going to claim to be ethical.

A change from a technology-centred to an other-centred conception of IT professional practice has the potential to re-orient professional practice in the discipline, to the benefit of the IT client base and beyond.

REFERENCES

- Alter, S. 2003, *Communications of AIS*, vol. 12, pp. 365-394.
- Armitage, W. D. and Karshmer, A. 2003, *IT Professional*, vol. 5, no. 5, pp. 37-43.
- Bruce, C., Pham, B. and Stoodley, I. 2004, *Studies in Higher Education*, vol. 29, no. 2, pp. 219-238.
- Critchley, S. 2002, Introduction. In *The Cambridge Companion to Levinas*, eds, Critchley, S. and Bernasconi, R., pp. 1-32. Cambridge University Press, Cambridge.
- Denning, P. J. 2001a, *Communications of the ACM*, vol. 44, no. 4, pp. 21-25.
- Denning, P. J. 2001b, *Communications of the ACM*, vol. 44, no. 2, pp. 15-19.
- Denning, P. J. 2004, *Communications of the ACM*, vol. 47, no. 7, pp. 15-20.
- Denning, P. J., Comer, D. E., Gries, D., Mulder, M. C., Tucker, A., Turner, A. J. and Young, P. R. 1989, *Communications of the ACM*, vol. 32, no. 1, pp. 9-23.
- Denning, P. J. and Dunham, R. 2001, *Communications of the ACM*, vol. 44, no. 11, pp. 21-25.
- Denning, P. J. and Dunham, R. 2003, *Communications of the ACM*, vol. 46, no. 3, pp. 19-23.
- Finkelstein, L. and Hafner, C. 2002, *The evolving discipline(s) of IT (and their relation to computer science): A framework for discussion*. <http://www.cra.org/Activities/itdeans/finkelstein.pdf> (accessed December 8, 2007).
- Freeman, P. and Aspray, W. 1999, *The supply of information technology workers in the United States*. <http://www.cra.org/reports/wits/cra.wits.html> (accessed December 8, 2007).
- Gorgone, J. T. 2001, *ACM SIGCSE Bulletin*, vol. 32, no. 2, pp. 11-12.
- Iansiti, M. and Richards, G. L. 2006, *Antitrust Bulletin*, vol. 51, no. 1, pp. 77-110.
- Kaarst-Brown, M. L. and Guzman, I. R. 2005, The IT professional: Who is "the IT workforce"? challenges facing policy makers, educators, management, and research. In *The 2005 ACM SIGMIS CPR conference on Computer personnel research SIGMIS CPR '05*.

- Kling, R. 2003, *Information Technology & People*, vol. 16, no. 4, pp. 394-418.
- Koehn, D. 1994, *The ground of professional ethics*, Routledge, London.
- Lenox, T. L. and Woratschek, C. R. 2003, *Information Systems Education Journal*, vol. 1, no. 45, pp. 1-18.
- McGuffee, J. W. 2000, *ACM SIGCSE Bulletin*, vol. 32, no. 2, pp. 74-76.
- Orlikowski, W. J. and Iacono, C. S. 2001, *Information Systems Research*, vol. 12, no. 2, pp. 121-134.
- Pham, B., Bruce, C. and Stoodley, I. 2005, *Higher Education Research & Development*, vol. 24, no. 3, pp. 215-232.

ACKNOWLEDGEMENTS

The material in this paper is a product of ongoing doctoral studies at the Queensland University of Technology, Brisbane, funded by a university Research Capacity Building Award (RCBA).

COPYRIGHT

Ian Stoodley and Christine Bruce ©2008 The authors assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

The Gamer's Dilemma:

An analysis of the arguments for the moral distinction
between virtual murder and virtual paedophilia

Morgan Luck,

School of Humanities and Social Sciences,

Charles Sturt University,

New South Wales, Australia.

ABSTRACT

Most people agree that murder is wrong. Yet, within computer games virtual murder scarcely raises an eyebrow. In one respect this is hardly surprising, as no one is actually murdered within a computer game. A virtual murder, some might argue, is no more unethical than taking a pawn in a game of chess. However, if no actual children are abused in acts of virtual paedophilia (life-like simulations of the actual practice), does that mean we should disregard these acts with the same abandon we do virtual murder? In this paper I shall outline several arguments which attempt to permit virtual murder, whilst prohibiting virtual paedophilia.

COPYRIGHT

Morgan Luck ©2008 The authors assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

Critical perspective on Ambient Intelligence technology

- ethical and societal issues-

Philippe Goujon

Facultés Universitaires Notre-Dame de la Paix -Computer Science Department
Namur- Belgium.

Partner of the MIAUCE project (www.Miauce.org)

Email : philippe.goujon@info.fundp.ac.be

Abstract:

The proactive and Aml technology into highly sensitive environment produces specific challenges that are inextricably linked to ethical and societal issues. Proactive systems such as Aml will make decisions without direct human supervision placing the technical system in a position of authority. The ethics of interactive computer systems that focuses on how such systems are (or can be) used by human users have been discussed at length, taking in account the possibilities of the technology presented in the project, it becomes urgently necessary to consider the implications of decisions made or influenced by computers. As specified by L Venter, MS Olivier and JJ. Britz "the integration of mobile technology, wireless networks, ubiquitous computing and artificial intelligence with thousands of embedded devices such as sensors and actuators may result in networks that can proactively monitor and respond to human behavior without human interaction and with little supervision. Decisions that can influence or alter the environment will be made at faster-than-human speeds." (Venter et al. 2005) Ethics as applied to current interactive computer systems will not be adequate.

The objective of this article is to analyze the ethical and societal problems related to the Aml technology. To reach that objective, we will firstly analyze the conditions for a critical perspective, then the ethical references used as the foundation of our analysis and in the last part of this article the ethical issues raised by Aml.

Keywords:

Ambient intelligence- ethics - critical perspectives – autonomy –responsibility – privacy – profiling – ethical principles.

Introduction: Information society, technical development and ethics

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology (Bruce Schneier).

The impact of techno-scientific developments on societal evolution and lifestyles no longer needs to be demonstrated. The profound transformations that have taken place in the last few decades equally involve energy, transportation, construction, telecommunications, administration, medicine, pharmacy and agricultural sectors. These transformations are closely linked to techno-scientific developments and particularly to stunning developments in Information and Communication Technologies (ICTs). However the information society emerging in the contemporary period can no longer simply be considered as a result of technical mutations. Up to now, this on-going global phenomenon that is technological, economic, political and cultural, is in search of a social and a political project, references and reaffirmed values. We are faced with the task of building networks

based on a cultural model incorporating clear collective choices, so that the principles of democracy are transferred on line – hopefully without loss - in the future.

The evolution of ICT is driving our society towards situations and applications where the humans interact so deeply with the "intelligence" pervasively distributed among them that at some point we will reach a divide where a fundamental choice will be presented to us: to develop a "utopian" environment where all humans will have access to an empowering and accessible techno-environment ("Ambient Intelligence environment") or head towards a "dystopian" environment where Bentham's panopticon⁶ will become more and more a reality thanks to thousands of sensors, computers and networks that will track every human movement. David Lyon called this new form of 'cooperative surveillance' 'Synopticon' and 'Scopophilia' (D. Lyon, 2003, 2006). The notion goes beyond Bentham's Panopticon and was interpreted by Zygmunt Bauman as a significant trend of the globalisation process.

In a world that is becoming increasingly homogenised, any capacity for questioning is likely to be stifled by the rational constraints extended to all fields. This brings us back to the question of the possibilities and the place of ethics within this framework of corrective regulation. The need for serious attention to the problem of allowing the conditions for the development of a responsible information technology is strong. It is based on the conditions for developing what is sometimes referred to as Value Sensitive Design, which recognises that any technology and/or artefact (i.e. ICT) embeds moral values into their technological design, research and development. A wider approach in evaluating emerging technologies should include not just the legal dimension (often referred to in the ICT field as "compliance") but also the ethical dimensions.

Conditions for a critical transformative room⁷

What we propose is to review the state-of-the-art in respect of the ethical analysis of ICT developments and in particular of Ambient Intelligence applications. Practically, the main problem consists of a deep lacking of background: the strong push for technology development too often obscures the need for any deep ethical consideration before a technical project is funded, developed and deployed. Some efforts have begun to consider ethics and ICT in the Ami domain that adopt different approaches: analysis from scenarios (e.g. PEACH), or "ethical review" panels (set up after the project has started, e.g. MINAmi⁸) consisting of "ethical experts" – who may come from a completely separate community. The "technical" community is typically separated from the "ethical" community⁹. One of the reasons for this separation is the specialisation of high-level studying (e.g. universities) where the "technical" study plan of engineers is very different from the "humanities" subjects of other faculties.

A more interdisciplinary approach is strongly required¹⁰. Indeed some technical universities are introducing in Europe some areas like "Science, Society and Technology" for engineers or "Computer Ethics" for computer scientists but not always as a mandatory component. Scientific projects can raise ethical questions, evidenced by the rules and procedures of the European Commission for the systematic ethical evaluation of projects submitted for funding in FP7. However, the elaboration of ethical standards is made uneasy by the common dividing line which still separates the justification of norms and their application. Yet, these two levels ought to be integrated if one considers the issue of ethical universality, which has to be newly analyzed within

⁶ The famous Panopticon was designed by Jeremy Bentham, British jurist and philosopher, towards the end of the eighteenth century. It is a type of prison, also known as the 'Inspection House', which enables an observer to watch all the prisoners without their knowledge. This essential principle of construction is reflected in the Greek neologism, pan- meaning 'everything' and - opticon concerning 'vision', and as such the word is meant to express 'the all-seeing place'.

⁷ Concept of critical transformation room from Crutzen 2003. Critical transformative rooms are characterized as those interaction worlds, where actions of questioning and doubt are present, which have the potential to change habits and routines, where the "change of change" has a differentiated potential

⁸ MINami (Micro-Nano integrated platform for transverse Ambient Intelligence applications, an FP6 project).

⁹ For example noted in the Human Report Ethical Audit produced in December 2004 (Editors: Peter Goldie, Sabine A. Döring and WP10 members). <http://emotion-research.net/deliverables>. Humaine (Human-Machine Interaction Network on Emotions) was an IST FP6 project.

¹⁰ There is some recognition of the interdisciplinary problem which has resulted in the PEACH project (FP6 Coordination Action on Presence) that includes a Working Group on social impact, legal issues and ethics. The approach taken is to analyze social impact scenarios and raise and address potential ethical issues. <http://www.school.peachbit.org/>.

the context of a multi-cultural Europe¹¹. The reflexive articulation of ethical norms and cultural contexts raised many problems among which are in first place the conditions of a reflexivity;

This is natural since the researchers and technical developers of Ami systems focus mostly on the technical and economics challenges before them, and are not usually aware of potential ethical issues when they don't consider ethical considerations and analysis as an obstacle to the technical and economics development. In short the problem we must first analyse is not so much to determine solution to ethical problems that to settle the conditions for raising ethical questions and for a new approach authorizing a real reflexivity and allowing a questioning on the integration of ethics in complex technical systems. Reflexivity may be defined as the capacity of actors and institutions to revise basic normative orientations in response to the evolution of economic, techno-scientific or political systems and to shortcomings in current modes of regulation. This reflexivity is not given, however, as is clearly shown by the growth of science and technology. Obligation of the economic constraints, interests concerned the influence of the experts, impression of the ineluctability of the technical projections, requests social, needs for the consumers. make that it becomes increasingly difficult to define the conditions of a critical perspective respecting the morals autonomy requirements of the thought.

The danger and problem is to limits the debate to the scientific perspective alone (hence the importance of expertise, and the tendency among politicians to favour traditional, "top down" governance of activities in which risks are involved) and, in shunning an approach based on technology assessment, or debate on the meaning and the ethical, cultural and social stakes. Instead of initiating an inclusive debate on the nature of the different forms of knowledge and vision of world, discussions limit the debate by adopting a positivist and, more often than not, reductionist approach that leads to cognitive closure. Hence the question of how to decompartmentalize ethical discourse and make it play a more important role in the joint construction of technologies? How to transcend the neo-classical, technological approach (the cost-benefit approach for Slovic)?

The economists' answer appeals to the industrialists, for it confirms them in their practices and habits. Hence again—even if, as Ulrich Beck has stressed, this is a perspective that needs qualifying—the difficulty of controlling the rampant growth of technological innovations politically; often as not, political institutions make do with furnishing them with a regulatory and financial framework within a dynamic system accompanied by positive feedback that leads to overheating.

In this context, expertise, be it philosophical or scientific, becomes the indisputable new source of normativity¹², and the problems revealed are confined to a scientific perspective alone—which means that the problems taken into account are confined to the realm of strict scientific rationality, and democracy is confiscated. There's a big risk that the possibility of genuine reflexivity, will be stifled by a technological and scientific rationality imposing its value system with as a result a dismissal of the prestige of the moral reason.

The stake is of importance, indeed various sectorial ethics tend increasingly to reinforce social differentiation characteristic of modernity by proposing an internal, and specific, framing moral problems, with the risk to exclude other external and alternative framings. As a consequence ethics is disconnected from the design of technological device and the lack of a concrete grid of assessment concerning the embedding of ethics in technological development makes this issue important. As a result ethics is often an "add-on", a sort of accessory and instrumentalized guarantee and not properly integrated neither understood in its methods and objectives which are clearly very different from the method and objectives of sciences and techniques.

Consequently, there is a strong need for the inclusion of ethical consideration before, during and at the end of a project technical and scientific, so that the technology 'incorporates' and tackles the ethical side (within its whole concept and implementation). In the Aml projects, which are fundamentally technical and scientific projects, this problematic is fundamental since the ethical and societal approaches aimed to influence the development and the design of the technical systems. A moral freedom of positioning is fundamental, it remains to question its possibility, and conditions.

¹¹ In Search of Common Values in the European Research Area, Pieter JD Drenth Ludger Honnefelder Johannes JF Schroot Beat Sitter-Liver, Editors. ALLEA – ALL European Academies, Netherlands.

¹² Normative is contrasted with its antonym, positive, when describing types of theories, beliefs, or statements. A positive statement is a falsifiable statement that attempts to describe ontology. A normative statement, on the other hand, is a statement regarding how things should or ought to be. Such statements are impossible to prove or disprove, thus forever banishing them from the world of the scientific.

The autonomy of the technique in question and legitimacy of ethics

When the cult of knowledge is replaced by that of the performances, moral, ethical and societal considerations are apparently private of justification. This is a consequence of the fact that conditioned by the technical framing we have forgotten that technique is not neutral. It is a manner of thinking, of making, and of transforming the world which is indissociable of the policy and, by the subjacent choices of ethics. From this point of view, the data processing and the techniques of the communication including the Aml are not neutral and *reflect*, in their constitution and their use, expectations of the society and are influenced by their socioeconomic context. For example, technological innovations that focus on satisfying needs of individuals also come to fulfil a function dependant on the cultural features of the society in which they fit. As in any society, these needs can be seen as negative or positive, for instance, perhaps negatively to control, or more positively to align the political, social and institutional goals with the individuals' desires (Lyon, 1993).

On this view, the organisational life has to become increasingly rationalized and controlled and organisational control will be "less and less apparent and increasingly powerful" (H. Isaac and Mr. Kalika, 2001; W.J. Orlikowski, 1991; J.R. Barker, 1993). The organisational perspective of ICTs stresses that any technological innovation is not a neutral tool to increase the production, but "a tactic deliberated to increase the managerial capacity". These characteristics also apply in a broader social sense, with the result that the introduction of ICT also shapes social practice: "information technology has become a constitutive technology and partly constitutes the things to which it is applied. It shapes our discourses, practices, institutions and experiences in important ways" (Van den Hoven, 2007).

Non-neutrality of Aml

This recognition of the non-neutrality of ICT should not be surprising, after all technology is designed with some purpose in mind guiding the technical direction. However, the implications of the technology in its capacity to affect and change social practices are not so easily seen. In the case Aml projects, the construction of the social legitimacy (and not just acceptability) of science and technology requires that the metaprinciples of normative nature subjacent with the action techno-scientist be considered. The technique is each time a historical and social project, and this project reflects the intentions which nourish a society, the interests which dominate it and the values which guide it.

In the case of the vision of Ambient Intelligence at a first glance it seems that it is based on technological progress in the fields of microelectronics, communication networks and interfaces. Nevertheless, it is also driven by socio-economic factors that go beyond the technologies alone (economic neoliberal rationality, rationalization of the production, demographic conditions, impact of terrorists actions, consumerization of the communication).

For a critical perspective

Every technical object is a construction which rests on some *a priori*. The political impact of a technique cannot thus be assigned to this technique alone, but must be allotted to the techno-speeches which diffuse it, give it a specific meaning and envisage for it specific usages. Data processing and the innovations related to the TIC, if they seem to be binding to the individuals, come, actually, to satisfy a need and to fulfil a function largely dependant on the cultural features of the society in which they fit.

It is only to the condition of recognizing the not-neutrality of the TIC that one can start to change his cognitive framing and can start to think to ethical and societal issues. Without this propaedeutics steps, one can just interpret the world and the technique in the restricted cognitive fields allowed by its framing in our case the technological framing with result or to negate any justification to ethical and societal consideration or to instrumentalize them and consider them as a mean to obtain a sort of ethical guarantee.

This recognition of the not-neutrality of the TIC returns realistic the ambition consisting to put instrumental rationality in perspective and to seek its political and societal control. The immediate urgency is to correct the manner of approaching the TIC corresponding at applying approaches which dissociate social approach from the technological one, political approach from economic and ethics, and too often privilege the response to the only economic, political and institutional constraints,.

The urgency is also not to limit ethics to the only question of the institution and the application of the standards. Indeed, such an ethics is purely a decisionist one. It refers immediately limits to the problem of the adequacy of the ethical representation to the context of action but ignores the origin and legitimacy of this representation a practical way to auto justify it and instrumentalized all ethical considerations. This problem is all the more important as from an ethical point of view, the theoretical image of human conveyed by a sphere of activity deserves, as underlined by Marc Maeschalck, "to be questioned according to its effective impact on the culture and the traditions. The extrapolation of a model of activity can become totalitarian when it claims to redefine the relation of human with its horizons". The function of knowledge in modern sciences is in an increasing way conceived in relation to the system of work. These sciences generalize and rationalize the technical capacity of human on the *objectalized* processes of nature and the society and the use of techniques of administration increasingly more effective and generalized.

Once the knowledge is reduced to the applied science, this type of science and rationality monopolizes the rational behaviour. The positivist conscience, consequently, combat like dogmatic any theory referring to the practice differently than those improving the possibilities of the practical applications. That means as a result that the practical (moral) questions become the object of a decision and are confined to the irrational field, unless they are not, in their turn, subjected to the only technical criteria of instrumental rationality as that is generally the case, "blocking any possibility of discussion on common ethical standards while imposing, preliminary a manner of understanding the world in general, a meaning of life determined usually inextricably by traditions, solidarity and personal identifications". The explanation is that the directives required by the action are divided into a rational determination of techniques and strategies and into an irrational choice of systems of values.

The consequence, for the economy governing the choice of the means, is a total freedom characterized by a decisionism in the choice of the highest goals (values associated with the action). However, as Ladrière underlines it, recalled by Maeschalck (...), "the decisionism is radically insufficient, because one cannot be satisfied to seek and pose principles of action and from that justify the action. It is also a question of permanently assessing the "ethicity" of the lived situations, i.e. of their particular relationship with the ethical requirements, themselves included/understood ideally like realization of the human one". It is the fundamental reason why what is ethically at stake is not so much to find an answer but well to make a room for ethical thinking to allow an ethical thinking that is to say an attitude that can localized the issues raised by technique and have the theoretical tool.

Without that ethical posture relying on ethical references, all the answers are useless since the cognitive tools to understand and apply them are not presents (the cognitive framing being in that situation still the technical framing.). The ethical step cannot be limited to provide the elements to establish the justification of a decision.

Ethics concerns convictions which are not explained in logic of compromise. A consensus can respect the interests of all the parts in question without being by its object or its purposes (industrial, economic, scientific) in conformity with the ethical requirements. The ethical provision precedes the consensual effort and is its only guaranty. But this provision is not obtained by negotiation, it refers to the intentionality of the actors, their relation to the real world, and their conceptions of existence and on which values those conceptions are founded.

In the field of subjectivity, the ethical interrogation is not satisfied by transformation of the individual forces into social autonomy. It seeks to exceed the responsibility concerning the measurable to open a reflection concerning the responsibility with regard to the non measurable, i.e. with regard to the destiny of humanity and the life and of our world. Compared to the life given, ethics is a concrete answer where a figure of humanity with its specific features is at stake. It thus answers partially in the concrete world to the challenges of a future for the human world. It cannot thus elude the specific fields of activities. Ethic answers the injunction of reality when it questions the rational choices for the management of the limits of our capacity of answer. It refers the human action to a destiny which exceeds it, that of the life which is "carried out" in it. Ethics must assumes a normative authority which wants to be free of any contextual constraints, otherwise ethics would be subject to the reign of instrumental rationality, and would transforms itself in a sort of justification for objectives that are not ethically founded but may be for example economically driven. Refusing to be subject to such constraints we assume, in that article, deliberately the normative authority of ethics.

The ethical interrogation refers to the construction of a human order and questions the way human are perceived and treated referring them to ethical references.

Ethical references

The human and social impact of technology needs to be considered. In ambient intelligence systems, the moral responsibility for the social impact of technology extends beyond just the practitioner. It concerns the society at large and needs a social debate. As underlined by Rob Meredith and David Arnott (jully 2003, p. 4) 'Whilst a large part of the moral responsibility for the use of technology belongs with system owners and users, it often falls to the practitioner, as a professional, to highlight potential ethical issues in proposed systems. Unfortunately, as underline by Conger & Loch many IT professionals lack the communicative skills, and the ethical training to be able to engage in an ethical dialogue (Conger & Loch, 1995)". Talking about ethics, the focus on responsibility is fundamental - ethics implies responsibility (without responsibility for an action residing with a person, then we cannot label the action (and its outcomes) as good, bad.

1.2.1 - Responsibility and moral autonomy

Moral Responsibility it is well known implies autonomy, without moral autonomy there is no possibility of responsibility. The action cannot be said ethical if justified and motivated by reasons dictated by the context (efficiency, security, profit, ...) The motivation of the action *must be, from the start*, moral (not conditioned by interest) So morality implies :

- 1) **moral autonomy**.... One can not reflect on the morality of an action in terms of its contribution to efficiency, security, profit ...
- 2) **Good Will**... to be ethical? The will to be moral!

In the case of informatics technological system, it is very often difficult to determine who is responsible for what. The determination of that locus will differ from project to project, system to system, issue by issue It seems apparent, however, that it is beholden on the IT practitioner, as an expert professional, to ensure that such issues are explored prior to, rather than during or after, an ethical dilemma, and that the relevant actors and decision makers are aware of their responsibilities. . However, where systems are designed to undertake actions autonomously of their developers, owners and users, or where a system contributes significantly to a decision made by a user, then a large range of potential ethical dilemmas might arise. This is of particular interest to computer scientists interested in the field of artificial intelligence. Lucas (2001) and Dowling (2001) both point out that Asimov was one of the first to codify a set of rules for autonomous systems, albeit fictionally, with his laws of robotics."

The other principle which is fundamental is according to the famous Hume principle that *values can never be infer from fact*. It is not because an Aml system is judged to be acceptable and answer to the legal requirements, that it is ethically and morally legitimated... Moral and ethics are fundamentally teleological - teleology here means that there are ends which are posed as objectives: the good life, the improvement of our current social and individual situation, respecting and promoting humanistic values, with the aim of protecting dignity, autonomy, preserving integrity of human being. It is necessary to keep that in mind when the societal acceptability of a technical system is considered to avoid reducing the acceptability problem to the acceptance problem. The acceptability concept implies the determination of the conditions that makes something acceptable (including the moral acceptability which can't be reduced to the acceptation according to the contextual constraints: politic legal economic...).

From those considerations it is obvious that concerning computer systems with a capability to take some decisions and cause action, the question of attributing a responsibility is highly problematic. More generally as underlined by Dowling, the concepts of autonomy, trust¹³ and responsibility become more problematic as the system is more active in the decision making process (Dowling, 2001).

Obviously, Aml can't apprehend ethical issues and so can't be by themselves responsible for their decision and action. What about their designers? Of course they are responsible, but there are many problems concerning the designer's responsibility: they can't be considered as the unique responsible since the informatics systems respond also to social economical political etc constraints. Moreover, many IT professionals lack the communicative skills, and the ethical training to be able to engage in an ethical dialogue (Conger & Loch, 1995). . It seems apparent, however, that it is beholden on the IT practitioners, as an expert professional, to ensure that such issues are explored prior to, rather than during or after, an ethical dilemma, and that the relevant actors and decision makers are aware of their responsibilities. But again one of the fundamental prerequisite for such an exploration is that those practitioners accept to free themselves from

¹³ The notion of trust has technical aspects as well as social, cultural and legal aspects.

their conditioning technical framing and have an ethical normative horizon as a reference. The other prerequisite are the ethical principles used as normative horizon.

Ethical principles

All ethical considerations need to have ethical principles reference. In the case of Aml where a decision is either made by the system, or based on the output thereof, Snapper (1998) suggests that the solution is to adopt a similar view to the situation where a physician relies on advice from non-computerised sources such as human consultants. In these situations, responsibility is shared amongst the various professionals. We agree, with Collste *et al* (1999) who highlight autonomy of the decision maker as important, but go further and point to the four principles of bioethics described in Beauchamp and Childress (1989): beneficence, non-maleficence; autonomy, and justice. The principles which Beauchamp and Childress employ in their approach are as put in evidence by very distinct from the Utility Principle and the Categorical Imperative.

“- Above all, these principles are not first justified through a specific ethical theory in order that they can then be – in a second step – brought to bear on moral experience.

- Instead, they are formed out of experience and in fact reveal a part of that experience.
- They are rules of thumb, or prima facie duties, which reflect the core stock of moral beliefs held in common in a modern pluralistic world. Principlism endows our ordinary moral experience (perception, intuition) with justificatory force. As Beauchamp and Childress emphasise, moral experience in general is a ‘credible and trustworthy’ source of ethical knowledge (Beauchamp and Childress 2001, p. 400). In that respect principlism is very different from justification in the framework of a Utilitarian or Kantian ethics, where one always needs to infer what one ought to do in a given situation. Instead we arrive at the Aristotelian idea that getting things right in ethical matters is much more a matter of seeing things right than of intellectualist justification.

The four principles of nonmaleficence, autonomy, beneficence, and justice constitute the least common denominator of morality. ” (Döring & Goldie)

A brief explanation of these principles in the context of biomedical ethics is provided in the following table:

Beneficence	= providing ‘benefit’ Beneficence obligates professionals to ‘do good’ towards their clients. It is their duty to further their clients’ welfare and interests. Beneficence seems relatively straightforward, but can be difficult to apply in practice. What exactly is a benefit? How can we tell whether a particular benefit will occur or not?
Non-maleficence	= ‘not harming’ Health professionals also have an obligation not to inflict intentional harm upon their clients, or to minimise a risk if it is necessary to take one at all.
Autonomy	Autonomy means ‘self rule’ or self-determination. That is, we all have the right to deliberate about our own values and make decisions about how we want our lives to go, free from the interference of others.
Justice	Justice requires that medical care be provided in the fairest possible way, treating ‘equals equally’.

Table 1- Tom Beauchamp and James Childress (2001) *Principles of biomedical ethics*, 5th ed. Oxford University Press, New York. ISBN 0195143329.

Those four principles are a useful tool for determining where the ultimate conflict in a problem might lie. Each of the four regulative principles should be regarded as guiding ideas for debate and decision making. These principles are open to competing interpretations and the precise relationship between each of the principles has to be informed by more general theoretical positions taken by the disputants. Deliberating with these principles means balancing them and specifying them to the particular case. Moral decisions also need virtues on the part of the moral agent to arrive at just decisions. Compassion, fortitude, and perseverance all affect outcomes.

In the case of Aml, we believe that there are enough parallels with general decision support systems development to argue that these four principles and their complements (dignity, integrity, and vulnerability) defined in the Barcelona declaration should apply there as well in the case of proactive technology, since it is this interpretation which is concerned by the project.

In the context of this article, we propose that these principles can be applied as follows:

- Autonomy refers to the right of the user to decide what should happen as result of a given situation.
- Veracity implies that the user knows exactly what information the system collects about the user.
- Beneficence is the expectation that the use of the system will be for doing good;
- “Nonmaleficence” is the expectation that the system will not be used with bad intent.
- Confidentiality ensures that the information collected by the system will not be freely available. Justice is the expectation that the system’s decisions will be fair.

Having as reference those ethical principles, in order for Ambient Intelligence to go behind the recurring one-sided claim that it will simplify our lives, save time, and liberate us from toil (Langdon Winner, quoted by Bohn *et al.* 2003), its societal and user implications should be made more explicit.

The problem with the visions that were proposed is that there are for most of them very optimistic. The portrayed everyday life in the scenarios that were proposed by scientist or industrials “is primarily a perfect life where users are able to cope, successfully, with their lives. Scenarios have a tendency to ignore the struggles, uncertainties and irregularities that are characteristic for everyday life as well. They are inclined to portray only the bright side of life” (Punie, 2003, p. 19).

As more and more objects and environments are being equipped with ambient intelligence technology, the degree of our dependence on the deployed devices is increasing accordingly. In a largely computerized future that is proposed, it might not be possible to escape from this sort of technologically with as a result an induced dependence, which leads to a number of fundamental social challenges for future ambient-intelligence systems.

More generally, the fact that these technologies will deliver personalised services to individual users means that somewhere a lot of personal information needs to be stored about those individuals. Such personal data can be used and abused. Thanks to data aggregators that gather and consolidate a wide range of information about groups – and individuals – in society, our government and commercial organisations already know a great deal about what we do and what motivates us.” However, without effective privacy protection measures, this brave new world of smart environments and interconnected objects could become an Orwellian nightmare” (Mattern, 2003; Bohn *et al.*, 2003; ISTAG, 2001). Addressing the balance between privacy and security will be a core challenge for the future of Ambient Intelligence.

For people to feel at home within Aml, it needs to be able to represent their multiple identities, respect their privacy and establish an acceptable level of security (Beslay & Punie, 2002). The questions that need to be tackled are in short: What kind of society is envisaged with Ambient Intelligence? How are the users configured in Ambient Intelligence? After having specified the condition for an ethical analysis and determined the ethical references, through a synthesis of the issues found in the literature, we will identify and try to analyze ethical and social implications of future ambient-intelligence landscapes. To try to understand human values, we need to consider numerous concepts including: behavior, trust, privacy, security, inclusion, social norms, respect, self-esteem, context, choice and control.

Ami ethical issues

The ethical issues of Ambient Intelligence

The evolution of ICTs is moving towards what is variously called pervasive computing, ubiquitous computing or simply Ambient Intelligence (AmI). The future scenario is of a computing infrastructure where the familiar "machine" (keyboard, screens, etc.) will disappear and will be distributed "around" us. The environments around us will include sensors and wireless devices able to detect human presence, to collect data on human parameters (physiological parameters, pressure, temperature, etc.), to detect situations that need attention from other parties, and react to human presence. These "future computing" scenarios represent a large-scale transformational change in the history of computing and are encouraged by the European Commission as demonstrated by the large number of AmI projects currently being funded. The significant opportunities of AmI recognised by the EU in the 7th Framework Program mainly refer to:

- Improving living arrangements for people and further supporting society to bring added benefits.
- Modernizing the European social model particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services.
- Improving Europe's economy in terms of: supporting new business processes; increasing the opportunities for tele-working in the networked home; enhancing mobility and improving all forms of transport; supporting new approaches to sustainable development.

At the same time, there is an increasing recognition that technical development in the area of ICTs can have ethical implications concerning privacy, identity, freedom, autonomy, dependability, social acceptability, the question of informed consent, problems of discrimination, risks and complexity, exclusion, profiling¹⁴.

Since our environment will become aware, active and responsive, many applications will have the immense potential to bring benefit to our lives by improving our communication abilities, automating common tasks, assisting those with special needs to participate more actively in society. However these scenarios and envisaged applications have the potential to lead us to an Orwellian society where every person's action could be monitored and recorded. Privacy then is one issue, but it is not the only critical ethical issue arising from such scenarios. Other ethical issues include (but are not limited to): equality of access (digital divide¹⁵), increasing social pressure, user-centred design, and security.

From Vision to Users

Ambient systems are often referred to as being IT systems intimately integrated with everyday environments and supporting people in their activities. In the visions of ubiquitous computing the integrative ideal is one of invisibility: "Such a disappearance is a fundamental consequence not of technology, but of human psychology. Whenever people learn something sufficiently well, they cease to be aware of it. Computer scientist, economist, and Nobelist Herb Simon calls this phenomenon 'compiling'; philosopher Michael Polanyi calls it the 'tacit dimension'; psychologist TK Gibson calls it 'visual invariants'; philosophers Georg Gadamer calls it 'the horizon' and the 'ready-to-hand'; John Seely Brown at PARC calls it the 'periphery'. All say, in essence, that only when things disappear in this way are we freed to use them without thinking and so to focus beyond them on new goals."» (Weiser, 1991) In 1998, Weiser coined the term "Calm Technology" in order to honour the fact that what he wished for the future was to focus on designing technology that would act in the periphery for us. (Weiser, 1998)

¹⁴ For example: Johnson, D. G., (2001), *Computer Ethics*, 3rd ed. Prentice Hall. Hamelink, Cees J. (2000) *The Ethics of Cyberspace*. Sage Publications. Spinello, R., (2000) *Cyberethics: Morality and Law in Cyberspace*. Jones and Bartlett. Tavani, H.T. (2004) *Ethics and Technology: Ethical Issues in Information and Communication Technology*. John Wiley and Sons. SWAMI, "Safeguards in a World of Ambient Intelligence (SWAMI): Pasi Ahonen et alii, final report, Deliverable D4 30 August 2006.

¹⁵ The digital divide y refers to the gap between those that have access to the new ICTs (internet or any emerging new technologies) and those that don't and to the disparities regarding the ability to use them.

The transition from ubiquitous computing to calm technology is mainly a transition from technology-centred work to human-centred work. The idea of invisible technology is strong within the calm technology perspective, as is the idea of fitting technology to the visible parts and the invisible parts of the iceberg that is used as a model of a human being. In this vision, human needs are positioned centrally and technology is seen as a means to enrich our life.

Aml visions: an utopie?

The ubicomp and Aml vision is to fully computerize society, with the objective to serve with its orientation towards the public as well as the private, the personal as well as the commercial, people in their everyday lives, functioning invisibly and unobtrusively in the background and freeing people to a large extent from tedious routine tasks improving of people's quality of life. Aml sees the human user as the main actor, always in control, playing multiple roles in society. We can note with J. P. Allen (Allen, 2004, pp. 7-16) the paradox at the same time attempting to maintain user control of a technology and make that technique invisible to the user.

Regarding the question of the autonomy, it is obvious for a proactive system, that, by its very essence, it limits the users' full autonomy (this raises a central ethical problem if we agree that personal autonomy is seen as being fundamental to our value as human beings)¹⁶. What will remain as cognitive possibility if the environment does not cease being built and in the same time to build a predetermined and finalized meaning? In this context the constructivist idea of a construction of reality must be put in question. Virtuality is a new philosophy, a new relation to the world, to reality, which is more significant, because the virtual concerns metaphysics. As very well underlined by Theodore Roszack (Roszack, 1994, pp. 11-14) "We think with ideas, not data. Ideas must be there to contain data. Ultimately ideas generate data by defining problems, raising issues (...) thinking in the highest sense of the word has little to do with information, and still less to do with expensive information-processing machinery. It has everything to do with knowing how to deal with ideas. And that requires plain old-fashioned literacy—the ability to read, write, listen and speak with critical awareness. In the natural order of things, it is ideas—whether in the form of judgements, evaluations, interpretations, theories, beauties of form and structure—that take precedence over facts and figures

Without putting in doubt the good will and intention of the scientist and industrial that proposed the vision it should be noted that each new technique is accompanied with a positive discourse that gives a positive representation of it and always positives social changes are promised and promoted and finally gives one-sided promises of a better world. Even if they maintain that they are focused on human rather on technique, the problem with these visions is that they are for the most part, technologically deterministic and at the service of the stakeholders promoting the new technique.

Is it possible to believe blindness those visions which present in a sunny colour the impact of the Aml. ? The widespread implementation of the Aml vision would have a tremendous impact on our everyday lives and society. It is probably one occasion where the overused phrase 'paradigm change' is appropriate" because it implies a radical shift in such dimensions as the users of the technology, its incorporation into different spheres of living and working, the skills required, the applications and content provided, the scale and nature of the markets and the players involved" (Miles , 2002, pp. 4-9)¹⁷. Previous examples have shown that social and ethical regulation mechanisms have always lagged behind technological developments.

Ubiquitous systems hold the danger of increasing social pressure and the digital divide. Ubicomp has the potential to create an invisible and comprehensive network. The more options a bundle of devices offers to their users, the greater is the challenge not to get lost in an abundance of possibilities

Concerning the visions that are proposed through the mean of scenarios one immediate remark, this better life for the user that is foreseen is in fact the designers' view of what should be better in their own lives. In general, users have little to say in the process of determining what is good for them. The ethical principles, the values embodied in Aml systems can, for the most part, be transferred from their designers, whose intent and competence will determine in which way the systems will influence their user's lives. This explains that from ethical perspective, the just and fair decisions of the proactive systems foreseen would depend on its purpose and the way it is designed.

¹⁶ It is possible to distinguish three levels of Aml control:

- High: Aml acts on behalf of the person.
- Medium: Aml gives advice and proactive suggestions.
- Low: Aml executes the person's commands.

¹⁷ cited by Punie, 2003, p. 12.

Concerning the scenarios, we must recognize that describing scenarios is not an innocent activity and implicitly represents a framing process conditioning the representation of the impact of the technology (positive impact in the case of the scenario build by industrials for example or negative as in the case of SWAMI scenarios)..

The risk is that taking the objective of a “technology for user”, in fact the user disappears to leave the place to the value and conception of society promoted by the industrial, the scientist and the policy makers which promote the technique which is perceived without democratic deliberation as a way to resolve societal and economic issues (for example security issues...). This raised also the question about who is in control of the Aml system. How are the user's interests protected and how is it ensured that information is objective? Concerning that problem of the “user's representation” we can highlight two key problems in theoretical ethics: “On the one hand, the determination of reality which we should influence with our acting, and on the other hand, the determination of the subject to which these actions should be attributed and should intervene in reality. In certain sense we may say that reality diminishes with respect to its confrontational character, and hence becomes virtual, and there comes into focus the subject that is perceived by intelligent systems, always as a user stereotype, i.e. as a buying, sickly and travelling subject etc. To a certain extent the subject becomes weakened, and, moreover, the formation of its identity is impaired. This is because it has to above all manufacture its personality without the recognition and non-recognition of a present Other, and possibly without the development of those specific skills dependent on this confrontational experience with the world.”(International Review of Information ethics, Vol. 8 - December 2007)

There is also the risk that intelligent agents' functioning becomes a new 'black box' since it is not obvious to understand the algorithms used to get certain results, algorithms which themselves are not neutral¹⁸.

Current descriptions of both context awareness and intelligent agents tend to present them as neutral, i.e. not needing to adopt a position within social relations. This will be difficult to sustain when confronted with users and non-users in their everyday life, since the latter are not at all neutral.

Justifications of Aml

In most of the scenarios and visions that were proposed two justifications for the development of Aml technology are security and care. People in those scenarios and vision are most of the time presented in danger, vulnerable. As underlined by Crutzen, domestication of Aml will be forced by jumping on the bandwagon of some fundamental fears of the individual and society such as the present loss of security and safety because of terrorism, the necessary but unaffordable amount of care for the elderly (Braun 2004)¹⁹ or economic constraint. Those driver, even if they are important, can't by themselves be a justification to a systematic deployment of Aml to resolve what are fundamentally social issues and not technical issues.

To relay on security, care or economic drivers is to obey to a technological determinism that finally reduced all social problem to a technological one with the danger to impose the technological framing with as a consequence the rejection of other alternative perspectives. Hence the force of technocratic ideology, an unacknowledged domination that arises from the fact that it hides behind technological rationality. In this context, expertise becomes the indisputable new source of normativity, and the problems revealed are confined to a scientific perspective alone—which means that the problems taken into account are confined to the realm of strict scientific rationality, and democracy is confiscated and the “objectivation” of the world we experience in order to predetermine the form of the world we share.

It is precisely the danger we can see in the promotion of Aml. All the problems (security, care etc) are conceived as if the only solution was a technical solution without considering alternative solution and without raising the question of the proportionality²⁰ of this technical solution to the perceived risk²¹ and

¹⁸ for an explanation of the non neutrality of algorithm in computer systems see for example Jeroen van den Hoven (2007).

¹⁹ Cited by Crutzen 2006, p. 4.

²⁰ We emphasize the need to make a deliberate decision with regard to appropriate levels of privacy and security, of control and constraints.

²¹ Risk is a concept that denotes a potential negative impact to an asset or some characteristic of value that may arise from some present process or future event. Frequently in the subject matter literature, risk is defined in pseudo-formal forms where the components of the definition are vague and ill defined, for example, *risk* is considered as an indicator of threat, or depends on threats, vulnerability, impact and uncertainty.

danger²². Considering from that perspective, the security justification for Aml can be considered as “a symptom of the fact that we have become so hypnotised by the ‘need’ to find technical solutions to crime, terrorism, fraud and many other problems that we forget to ask whether these solutions are even appropriate, and whether there might be other, non-technological or less invasive answers” (Murakami Ball, 2006, p. 5). The last CNIL²³ annual report (CNIL, 2006) and to give another example an Australian report concerning video surveillance highlight that risk. (Parliament of Australia, 2005).

According to the Lisbon European Council of 2000 and the e-Europe 2005 Action Plan, the European Union is committed to developing, amongst others, ‘an information society for all’ and to enable all European citizens to benefit from the knowledge society. The Lisbon process clearly stated that the European knowledge based society should also be a socially inclusive one. This places notions of the digital divide on the policy agenda. It is of concern to policy makers that (new) technologies should not become a (new) source of exclusion in society. All this is perfect but the concept of information society is not defined and can be related to many visions (positive if it is driven by humanistic concerns more problematic if it is driven only by economic considerations which seek justification in societal considerations to assure the acceptance of the techniques developed.).

Jacque Berleur underlines that « the nature of eEurope action currently remains modelled by the obstinate classicism of a vision generated within inner administrative circles and seeking legitimacy through reliance on chosen expert groups, a vision translated into vague action plans and embellished with some social and democratic concerns. » « We cannot avoid thinking that social and societal considerations have been sprinkled on what mainly remains a market-driven plan. ». In our opinion, the market-driven option has never been questioned since it was chosen as a central pivot in the Delors White Paper... » (Berleur and Galland, 2005).

It is undeniable, that the policy makers are fascinated by the technique. The technique seems to them to offer the horizon of certainty that the ideologies and more generally the thought do not appear capable any more to provide. It operates in their perception a looping enters, on the one hand, their convictions of backgrounds increasingly conditioned by the impact of the infiltration of the technique in our epistemology and leading to social habitus and, on the other hand, interpretative and doctrinal outgrowths which contribute to solidify, by theorizing them, these forms of life and thus to reinforce them in their apparently inescapable character. A symptom of this tendency is the call to the technique in all the recesses of our public policies - education, health, environment, administration etc... - to solve the problems which affect our societies.

Again to analyse with an open mind the issues raised by Aml requires to changes of cognitive maps, a profound shift to human placed above technical, economic and politicians considerations, a good will that accept not to reduce all the problems to the technical and economic ones a good will that accept that the fundamental value of "autonomy" (with its associated values of integrity, dignity, and vulnerability) should be placed in the context of care for others - a context that already presupposes an ethic of solidarity, responsibility and justice (fairness). Without that necessary cognitive shift all ethical considerations are just mere justifications, a sort of label and guarantee to what has been decided *a priori* according to other constraints and necessity (mostly economic and technical ones), which is ethically unacceptable. Of course this shift can't be imposed; it must be a choice depending of a free will - that is why the expert approach is not sufficient and why the ethical approach implies a learning²⁴ and an effort which aims to allow an appropriation, by the stakeholders, of the ethical process. It is also an explanation why the ethical problems can't be resolved only by giving, from a top down perspective, solutions in a table²⁵ to ethical problems defined by the experts (it should be highlighted that waiting in that way external solutions is a way deny all ethical responsibility because it is a way to escape to the ethical requirement to take upon oneself the ethical process).

Most of the current day systems and application designs are unfortunately technology driven, the ethical and societal considerations serving more as a justification than really as a mean to develop a

²² danger is a keyword used to denote that an indicated action will result in serious personal injury or harm.

²³ CNIL, Commission nationale de l'informatique et des libertés.

²⁴ This justifies the necessity of those reflexions concerning the condition for a reflexive and critical perspectives.

²⁵ Ethical reflexion implies deliberations, critical discussion and is fundamentally a process which takes time ...

real reflexivity, since most of the time the system under development can't be refused. What is open to discussion is how to make that solution acceptable and ethics a way to seek an ethical justification. The care and security justifications that are advanced as justifications by the promoters of Aml can't be an insurance to counter-balance the risk of dehumanisation and depersonalisation by progressively reducing people to object and source of data for Aml systems. Honest citizens have a moral and democratic right not to be treated as criminals; otherwise, they will be unfairly victimized. The problem is that as underline by Wood David Murakami and Ball Kirstie (2006, p.3), we are already living in a surveillance society:

The surveillance society has come about almost without us realising. It is the sum total of many different technological changes, many policy decisions, and many social developments. So there has been very little public debate about surveillance. The surveillance industry is already massive and (especially since 9/11) is growing much faster than other industries¹²: the global industry is estimated to be worth almost \$1 trillion US dollars, covering a massive range of goods and services from military equipment through high street CCTV to smart cards. The surveillance society has come about often slowly, subtly and imperceptibly and by the unforeseen combination of many small paths into one bigger road. Wood David Murakami and Ball Kirstie (2006, p.3).

Aml and human representation: Profiling, privacy issues, and responsibility

The future of the brave new world spotted by Aml promoters is a world in which "intelligence" is embedded in virtually everything around us. « In promoting their vision of the future, Aml promoters follow the ideal of creating devices which cause no disturbances and fit perfectly with their assumed expectations. They are convinced that digital environments, by acting on their behalf, can improve of people's quality of life. » (Crutzen, 2006, p.3) This humanistic concern is somehow paradoxical because at the same time, in the promoter's vision of Aml, it is claimed that it is user-centred and seeks the mental and physical invisibility of Aml technique which means an increasing difficulties for the Aml users to be aware, to influenced and to control the systems and the values embodied in them.

"The overvaluation of 'design' by designers, industry and research has reduced 'design within use' to themes such as 'the adaptability of the technology' and 'the acceptance of these technologies by users'. This permanent adaptability raised numerous problems, including "the Knowledge Sustainability problem. In a highly dynamic world, the sustainability of knowledge risks being lost. Such a loss or accelerated devaluation of long term experiences could, in the long term, contribute to an increased uncertainty and lack of direction for people in society" (Jürgen Bohn, p.18).

The biggest price of the promised adaptability of these intelligent devices is without doubt continuous measurement and interpretation of our body²⁶ data and movements"(Crutzen, 2006, p.5).

Profiling and social sorting risk

Indeed, the adaptative environment, the realisation of the brave new world promised by the promoters of Aml techniques implies the efficient collect of data concerning human being and as a consequence first the risk of what David Lyon, Professor of Sociology at Queen's University in Canada, calls through profiling a "social sorting" – " the Categorizing persons and groups in ways that appear to be accurate and scientific according to some predefined ontology or values framing, but which in many ways accentuate differences and reinforce existing inequalities" (Lyon D, 2001) ²⁷ and secondly the opening up of the private lives of Aml users. We must also highlight the risk concerning the freedom. Indeed, profiles can limit freedom of choice of users by confining them within the limited set of options on offer by the providers. Profiles tend to govern opaque decisions about individuals concerning their access to services, such as obtaining credit or a position. This opacity implies the non negligible risk that this profiling activities induced a sort of cognitive closure due to the positive feedback consisting in the marketing field in giving more offer to the consumer according his preference, which mean that the consumer's cognitive openness is automatically, progressively and in an insidious way conducted to be "restricted" to his preferences.

Profiling activities are essential in order to achieve the objectives of an *adaptive behavior of systems in response to the user's mental or emotional state and action in order to delivery services to users and*

²⁶ '... for investigating different forms of natural, multimodal human-computer interaction. It involves the research and development of computer vision, speech and gesture recognition systems that connect media and physical spaces to what its inhabitants are, and do and say.' (Cantoni Rejani 2004)

²⁷ Lyon D (2001) cited by Bohn Jürgen et al., p. 18.

facilitate his life. Profiling activities implies a continuous measurement and interpretation of our body data and movements. This profiling activity poses a clear threat to personal privacy above all if it is mentally and physically invisible and unobtrusive, a threat that is the price of the promised adaptability of these intelligent devices.

This threat concerns obviously the problem of the control by the user, that is to say by the people who will be monitored by the system, on the collection of data that were taken from them. Everyone should have the possibility to know which personal information is stored, why. The article 8 "Protection of personal data" of the Charter of fundamental human rights of the European Union (2000) summarizes important principles concerning the protection of privacy and the processing of personal data²⁸. According to article 8, processing of so-called sensitive data ('personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life') is principally prohibited, unless the data subject has given explicit consent.

The danger of invisibility

As the Aml seeks to be invisible it is foreseen that the collect of data will be able to be done without the consent of the users. This invisibility, which is a technological design statement raised many problems the most obvious one is that the power of control will be invisible. The consequence is a danger that the users will have less and less opportunities to adjust Aml devices to protect themselves from unwanted actions transforming human in objects of the systems reducing their responsibility and autonomy, including moral autonomy since the value directing the systems interpretation and action will not be chosen by the user but imposed by the designers of the systems.

We highlight that the Artefact physical Autonomy will be also reduced. Networked everyday objects embedded in an ambient- intelligence landscape loses part of their autonomy and, with this, exhibit an increased dependence on the infrastructure. For users, this reduces the "object constancy" of the objects that surround them (for example the necessity of a regular connection to internet to a server. May even make object more error-prone and less autonomous). The fact that Aml system will integrate object in a communicating network will raise also the accountability problem: If "autonomous" objects start taking decisions on their own, legal guidelines need to be drawn up in order to resolve who is ultimately responsible for these business transactions. This problem raises the question of who guarantees the objectivity and accuracy of the statements made. In a certain sense, Aml are becoming media representing a particular "ideology" (e.g., that of the product's manufacturer, or the politically motivated opinion of a consumer protection organization).

As remarked by C. Crutzen, "our body representations and the changes the individual will make in the environment could be unconsciously the cause of actions and interactions between the Aml devices, without knowing the reason of the reaction of the system."²⁹ Although 'not seeing this technology' could be counterproductive, it is suspicious that computing is largely at the periphery of our attention and only in critical situations should come to our attention. Who will decide how critical a situation is and who is then given the power to decide to make the computing visible again? Providing selective perceptivity to consumers could be counterproductive for the acceptance of Aml. Making technologies disappear, while assuming that this will reduce the tension for users could, on the contrary, make acceptance insoluble (Punie 2003, pp.40-41)."

In the same line of thought, the system can choose action at our own place without any possible feedback to correct the framing of interpretation and without our participation in the process of domestication the tool being invisible from the beginning and not becoming invisible through learning from the users (people monitored by the system). From that perspective, mental invisibility can't be reduced to physical invisibility since mental invisibility implies an integration process on the part of human actors. We have to underline here the problem of the Information asymmetry which positions the consumer or end user in an position of inferiority. This asymmetry of information is particularly

²⁸ The right to privacy is also consecrated by numerous national constitutions and by other international legal instruments, such as The Universal Declaration of Human Rights (United Nations, 1948) and the International Covenant on Civil and Political Rights (United Nations, 1966).

²⁹ 'The human actor should know ... why the system has reacted as it reacted' (Schmidt 2004) cited by Crutzen (2006, p. 14). The problem of accountability is here a crucial problem, of course the problem of giving person who is subject of Aml decision all the relevant information is a part of the solution but not all the solution because the problem and risk is to appealing to simply shift the responsibility and liability onto the end user

the allocation of functions, to use the iteration of design solutions, and to set up a multidisciplinary design team the "Design for all" standards for accessibility of information technology products promoted by the European Commission, the issue of user evaluation in ambient displays (e.g. Mankoff et al. 2003) or user-oriented definitions of context-awareness (Dey 2001). This finds an echo in the Report of the Science and Society Forum (2005) to the European Commission by Ulrike Felt which urges not to consider public influence and criticism with suspicion, rather to see it in its positive side: "Critical citizens do not hinder the transfer of science from the laboratory to society but play an essential role in this process. As a consequence, blind trust and consensus from the side of the public should not be perceived as the central goal to be reached by all means. The second perspective underlines the central function of epistemic citizenship in a knowledge society. If we take the idea of knowledge society seriously it requires the diversification of types of knowledge recognized as being relevant (...). It was further seen as crucial to give up the classical fact-value divide in public techno-scientific issues as it hinders more open forms of debates, and it is misleading about the fact that values are also embodied in expert knowledge. Public debates about science and technology in society are to be understood not so much as a battle between different forms of scientific knowledge, but rather as places where different visions and imaginations of the world are being negotiated." Most of these activities are probably mainly based on functional descriptions of how to involve users in the design process. This constitutes a first logical step, but the real challenge may lie in involving users in a sociological sense, i.e. by taking into account the micro-context of their everyday lives.

A challenge for adaptive computing and for Aml in general is to find an acceptable balance between openness and adaptability versus user guidance and rigidity. Perhaps the worst aspect of those Aml could be the impossibility to escape to the *normativity* of the system and, in a dystopia conception, be punished when trying to oppose to the implicit value framing of the systems and behind of its designers. The problem is again the possibility to control those systems and for the Aml in public space to decide democratically of their framing of interpretation and action, of the values embodied in them.

Being invisible the domestication of those systems can pose, apart from the privacy problem, some difficulties, as Punie underlined. "Exactly because they are invisible, they become uncontrollable (...) There is a difference between the physical and mental disappearance of computing, and it is incorrect to assume that physical disappearance will lead automatically to acceptance and use, and thus to mental invisibility... There is a substantial difference between these two perspectives, however. Aml assumes the material or physical disappearance of computing, while domestication refers to the mental invisibility of the technology. The two might exist together, but not *per se*: physical disappearance will thus not automatically lead to mental disappearance and hence to smooth acceptance and use of Aml. The former may even harm rather than facilitate acceptance, precisely because Aml is invisible and thus difficult to control"³⁴ Control and accounting mechanisms appears as important tools for determining who is in control of an autonomous system, and who is responsible if something goes wrong. This invisibility poses another problem. Whenever a Aml system causes damage, the complexity of the systems is likely to make it very difficult to find the cause. System behavior is determined by the interplay of numerous software products, hardware products, user interaction, network protocols, and so on. Here the causation principle comes up against limits because of a complexity created by humans that they no longer master (Hilty Lorenz *et al.* 2004, p. 866).

This danger is also related to another one which is the problem of an ambient intelligence divide and the potential exclusion³⁵ of a part of the population. Having more information opportunities does not necessarily mean more justice or freedom. To avoid this risk of exclusion it is a minimal prerequisite that accessibility is required in order to support the inclusive participation (user acceptance), awareness and learning of users with as subpoints equal rights and opportunities, usability (vs. complexity), training/education and the question of dependability which can be tackled by an effective implementation of Aml technologies by taking into account both technical constraints and harmonized human-machine interfaces.

³⁴ Punie, 2003, p. 38.

³⁵ As underlined in the opinion of the Committee on Employment and Social Affairs for the Committee on Industry, External Trade, Research and Energy on the proposal for a Council decision concerning the multiannual framework programme 2002-2006 of the European Community for research, technological development and demonstration activities - ambient intelligence systems offering access to the information society for all *regardless of age or situation*, as well as interactive and intelligence systems for health, mobility, security, leisure, preservation of the cultural heritage and environmental monitoring. *Intelligence systems should be particularly aimed at securing access for and participation by socially excluded and disadvantaged groups in society including disabled people; covering both design for all principles and assistive technologies in this field.*" (Mantovani Mario (draftman)):

In line with the problem of exclusion we must also put in evidence the question of the possibility to choose. Does the user will have the possibility to refuse the systems? To switch it off? To influence it? Again, there is a clear paradox in claiming that this technique is 'human-centered computing', user-friendliness, user empowerment and at the same time imposed it to the society, to the users without any possibility to influence it, to refused it. The problem is even more important since that technique acting and providing services represents also a value and to a certain extent and ethical framing which represent a certain conception (the conception of the designers of the scientist of the society³⁶ ...) of the world and of human, a conception that can't be accepted without deliberation that allow a reflexivity of the second order that is to say a reflexivity concerning the objectives off the system and its framing (ethical, societal etc..). Again without a possibility of changing of framing and of objectives the deliberative process is nothing more that a sort of game aiming at justifying what was already decided.

The privacy issue

There is the major problem of privacy. Privacy is not a simple concept. Nissenbaum (2004)³⁷ presents a model of informational privacy in terms of contextual integrity, namely, that determining privacy threats needs to take into account the nature of a situation or context: what is appropriate in one context can be a violation of privacy in another context. Nissenbaum describes the connection between privacy and autonomy: the freedom from scrutiny and relative insularity are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide freedom for people to formulate for themselves the reasons behind their choices, preferences and commitments. Thus, the privacy aspect called "utility", the right to be left alone, is much more than just a utility because it is important for personal development. Singer (2001) argues that privacy is not only about disclosure of dangerous information or disturbing a person at a wrong time or with information on a wrong topic. For example, personalisation of advertisements may seem to be beneficial. Instead of a bunch of useless and timerobbing advertisements about, e.g., new skis, a client who is not interested in skiing will receive advertisements about what he is truly interested in, for instance, new fishing rods. However, such personalised or targeted advertising may be not so innocent or beneficial in a long term because advertising views people as bundles of desires to buy more and more, and this view is partially true. Precise advertisements are harmful because they proceed to reshape human nature to fit the picture of "being a bundle of desires", diminishing people's capacities of reasoned choice and thoughtful action. Thus, Singers work also links privacy to personal development

A simple but useful definition of privacy is "the ability of an individual to control the terms under which their personal information is acquired and used" (Culnan MJ, 2000, pp. 20–26) As such, privacy is about individuals' capabilities in a particular social situation to control what they consider to be personal data. Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations. It is an interest that has several dimensions:

- privacy of the person. This is concerned with the integrity of the individual's body. Issues include compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilisation
- privacy of personal behaviour. This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places
- privacy of personal communications. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations
- privacy of personal data. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.

Table 2 - The several dimensions of privacy concept (COST 219 ter, p. 19)

³⁶ We have to evoke here the gender question which is crucial: industry claims that they apply female values and translate these into 'ease of use' see Manning Andre 2002.

³⁷ Friedewald Michael *et al.* (2005, p.5).

Harvard law professor Lawrence Lessig (Lessig, 1999) distinguishes between a number of motives for the protection of privacy in today's laws and standards

- Privacy as Empowerment. Seeing privacy mainly as informational privacy, its aim is to give people the power to control the publication and distribution of information about themselves
- Privacy as Utility. From the viewpoint of the person involved, privacy can be seen as a utility providing more or less effective protection against nuisances such as unsolicited phone calls or emails. This view probably best follows Brandeis' definition of privacy as "The right to be left alone," where the focus is on minimizing the amount of disturbance for the individual (Warren S, Brandeis L 1890).
- Privacy as Dignity. Dignity not only entails being free from unsubstantiated suspicion (for example being the target of a wire tap, where the intrusion is usually not directly perceived as a disturbance), but also focuses on the equilibrium of information available between two people: as in a situation where you are having a conversation with a fully dressed person when you yourself are naked, any relationship where there is a significant information imbalance will make it much more difficult for those with less information about the other to keep their composure.
- Privacy as a Regulating Agent. Privacy laws and moral norms to that extent can also be seen as a tool for keeping checks and balances on the powers of decision-making elite. By limiting information gathering of a certain type, crimes or moral norms pertaining to that type of information cannot be effectively controlled.

Table 3 - Motives for the protection of privacy³⁸

"The old sayings that 'the walls have ears' and 'if these walls could talk' have become the disturbing reality. The world is filled with all-knowing, all-reporting things" (Lucky R ,1999) Such comprehensive monitoring (or surveillance) techniques create new opportunities for what Gary T. Marx calls border crossings (Marx GT 2001) He distinguishes four different border crossing (see table 4).

* Physical borders of observability, such as walls and doors, clothing, darkness, and also sealed letters and phone conversations. Even facial expressions can represent a natural border against the true feelings of a person Social Borders³⁹. Expectations with regard to confidentiality in certain social groups, such as family members, doctors, and lawyers. This also includes the expectation that your colleagues do not read personal fax messages addressed to you, or material that you leave lying around the photocopier.

* Spatial or Temporal Borders. The expectation by people that parts of their lives can exist in isolation from other parts, both temporally and spatially. For example, a previous wild adolescent phase should not have a lasting influence on the current life of a father of four, nor should an evening with friends in a bar influence his coexistence with work colleagues.

* Borders due to Ephemeral or Transitory Effects. This describes what is best known as a "fleeting moment," a spontaneous utterance or action that we hope will soon be forgotten, or old pictures and letters that we put out in our trash. Seeing audio or video recordings of such events subsequently, or observing someone sifting through our trash,

³⁸ motives for the protection of privacy from Bohn Jürgen et al., web reference: <http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf>

³⁹ In the case of emotion recognition, the expression of natural border crossing is really adapted. Indeed the system infers the emotion we feel from our face expression and crosses the physical border to infer from the exterior expression of the face the emotion which represents fundamentally an inner state. This emotion recognition and determination can be perceived as an intrusive determination and a sort of privacy violation. Who has the right to tell what I feel , without my consent and without possibility to correct the interpretation?

would violate our expectations of being able to have information simply pass away unnoticed or forgotten.

Table 4- Four different border crossings that form the basis for perceived privacy violation Natural Borders

Putting ambient-intelligence systems into place will most certainly allow far greater possibilities for such border crossings in our daily routines (for example the hypermnésie problem in the case of marketing profiling, social crossing when for example have information concerning a relative without his consent and natural border crossing when one will be able to see your actions behind closed doors or determine your emotion from your face expression...) and represent an undeniable threat for our privacy. Privacy is a hard problem because individuals wish to control their personal information in a very detailed and nuanced manner.⁴⁰ Goffman (Goffman 1961) noted that people must control their presentation of self, their face... People need to be able to control what others think of them, and find it disconcerting when they cannot. Culnan and Armstrong (Culnan MJ, Armstrong PK 1999) make the argument that people have two kinds of privacy concerns.

- First, they are concerned over unauthorized access to personal data from security breaches or the lack of internal controls.
- Second, people are concerned about the risk of secondary use; that is, the reuse of their personal data for unrelated purposes without their consent. This secondary use includes sharing with third parties who were not part of the original transaction.

It also includes the aggregation of transaction data and other personal data to create a profile with all the risk connected to the problem of identity⁴¹ recognition and localization and spamming⁴². Smith et al.⁴³ raise two additional concerns: people have a generalized anxiety about personal data being collected, and people are also concerned over their inability to correct any errors. It should be possible for a person to control the information profile that has been monitored within an ambient intelligent system. The moral requirement is therefore, that it must be possible for persons to control and make choices concerning the functioning of ambient intelligence. This is an implication of the moral principle of autonomy.

The invasive potential of Aml is, nearly by definition of the Aml itself, great. The Aml can fulfill their functions of proactive device indeed only by the mean of data collect from individuals and their action emotion etc...in determined context. "Most people would be shocked to find out just how much information they consider private is already in the public domain," says project information coordinator David Wright of Trilateral Research & Consulting in London. "This might poses severe risks to privacy and issues concerning the use that can be made of those data".

It must be underline that the best and the most efficient solution, from a technical perspective, concerning the collect and processing of data to provide a service, a care or to assure security is not always the more morally acceptable (even if it is accepted by users...). According to Wright Because of threats to our society, most people are willing to compromise on their personal privacy in order to gain greater security. Yet – is our security actually better than before we gave up this privacy. From an ethical perspective there is a great problem here since the threat is more susceptible to be acceptable under security menace or it is exactly the same problem as for example in medical testing the consent can't be obtain when the subject is subject to a constraint (example economic constraint).

Ethically the consent implies the moral autonomy of the person. Informed consent defined by ask-it project consortium, is the process by which a participant will be fully informed about the research in which he/she is going to participate. It originates from the legal and ethical right the participant

⁴⁰ Every data collected must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified

⁴¹ This identity issue has been systematically analysed by the FIDIS project.

⁴² The risk of spamming encompasses several issues such as profiling, disclosure of personal data and malicious attacks. Different facets of spamming, such as false alarms and blackmail, are referenced in scenarios one, two and three.

⁴³ Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy. measuring individuals' concerns about organizational practices. MIS Quart 20(2):167–196

or end-user has to know and to control what happens to his / her body and personal data and from the ethical duty of the owner of the system to inform the end-user consumer.... Seeking the consent of an *individual reflects the right of an individual to self-determination* and also his/her fundamental right to be free from (bodily) interference, whether physical or psychological, and to protect his / her personal data. These are ethical principles recognised by Law as legal rights. A distinction between three informed consent elements is possible: the information given, the capacity to understand it and the “voluntariness” of any decision taken. Respect for persons requires that participants, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided, when adequate standards for informed consent are satisfied. Informed consent is a process, not just a form. A related issue to that consent concept that has to be resolved is how to advise people when their actions are being monitored ... When should notification be mandatory? How can users be effectively signalled? Given individual differences in sensitivity and awareness, it may be difficult to provide adequate notification to some without annoying others (NRC/NAS 2001 pp. 135f.).

It is the same for the question of the moral acceptability which must free itself from all contextual constraints (otherwise in an insecure context everything would be acceptable and justified - the USA patriot act is a paradigmatic example of that danger).

With ambient intelligence systems, it is easy to foreseen not only an augmentation in the quantity of privacy issue but the occurrence of some qualitative changes:

“First, current legislation, although it claims to be technology neutral, is somewhat biased towards existing technical solutions, like personal computers, large displays, keyboards, and web pages. For example, according to the European Directive on privacy and electronic communications (2002/58/EC), services must provide continually the possibility, of using a simple means and free of charge, of temporarily refusing the processing of certain personal data for each connection to the network or for each transmission of a communication. It would be quite easy to fulfil such requirements with a PC based system, but very difficult with a tiny Aml device which has a minimal user interface. Second, people’s notion on privacy is changing. We are already getting used to the idea that while we are using for instance Internet services, someone can be able to observe our doings. While travelling abroad, we need to frequently present our passports and other documents, even though it makes it possible for authorities to follow our paths. In the past, that was not possible, but still most people are not concerned about the change. Either they accept the reduction of their privacy, because they think it is necessary or that they get something valuable instead, or they do not care. Anyway, it seems that most people will not object the gradual impairment of their privacy. The expectations of privacy are very much related to the surrounding culture and social norms and as they slowly change, people will also have a different notion on privacy.” (Pitkänen Olli and Marketta Niemelä, pdf p. 7).

According to Jürgen Bohn et al.(Bohn et al.) "having thus both monitoring and search capabilities at the very core of their architecture, ambient-intelligence systems will very likely provide their developers, owners, and regulators with a significant tool for driving the future development of privacy concepts within society".

Apart the privacy issue, we must not neglect that there are people who simply do not like this vision as it is presented by the Aml promoters, regardless of privacy. This will also be a great challenge for the supporters of Ambient Intelligence.

Synthesis

The strong push for technology development too often obscures the need for any deep ethical consideration before a technical project is funded, developed and deployed. To take an active critical part in the technological design of our daily behaviors means to deconstruct meanings, especially the oppositions that can be found in the discourses of Aml designers and computer

In the case of Aml, the construction of the social legitimacy (and not just acceptability) of science and technology requires that the metaprinciples of normative nature subjacent with the action techno-

scientist be considered. It is only to the condition of recognizing the not-neutrality of the TIC that one can start to change its cognitive framing and can start to think to ethical and societal issues.

The urgency is to limit ethics to the only question of the institution and the application of the standards. Ethics is never in the answer (always conditioned) but well in this dynamic movement of questioning, before the action and on a border, that which separates our subjective existence (with its presupposed, its preferences, its convictions, its hidden motivations) from the constraining externality. What is ethically at stake is not so much to find an answer but well to make a room for ethical thinking to allow an ethical thinking that is to say an attitude that can localized the issues raised by technique and have the theoretical tool. The ethical interrogation refers to the construction of a human order and questions the way human are perceived and treated. The fundamental prerequisite for such an exploration of the ethical problems raised by a technique is that the practitioners of that technique accept to free themselves from their conditioning technical framing.

Ethics implies responsibility, autonomy and good will and is fundamentally teleological. Ethical ways of thinking need to be encapsulated within the very process of the research itself, probably based on multi-disciplinary or interdisciplinary perspectives. A more informed and balanced analysis of the potential social and ethical implications of technology would, it is hoped, be the result.

We have determined as ethical references needed for our ethical exploration of the ethical issues raised by Aml: nonmaleficence, autonomy, beneficance, and justice, dignity, integrity, vulnerability.

References

- Allen, J. P. 2004, The Social Analysis of Ubiquitous IT in *Challenges for the Citizen of the Information Society*, edited by Bynum, T.W., N. Pouloudi, S. Rogerson and T. Spyrou, ETHICOMP 2004. pp. 7-16.
- Ambient Agoras: Dynamic Information Clouds in a Hybrid World IST-2000-25134 - D15.4 – European Disappearing Computer Privacy Design Guidelines v1. WP15 – Privacy Issues
- Barker, J.R. 1993, Tightening the iron cage: concertive control in self-managing teams, Administrative Science.
- Beauchamp, TL, & Childress, JF 1989, *Principles of Biomedical Ethics*, 3rd edn, Oxford University Press, New York. and 2001, *Principles of Biomedical Ethics*, 3th edn, Oxford University Press, New York.
- Berleur J. and Galand J.-M. 2005, ICT Policies of the European Union : From an Information Society to eEurope. Trends and visions, Excerpt from Jacques Berleur and Chrisanthi Avgerou, Eds., *Perspectives and policies on ICT in Society*, Springer Science and Business Media, 2005.
- Beslay, L. & Punie, Y. 2002, 'The virtual residence: Identity, privacy and security', The IPTS Report, Special Issue on Identity and Privacy, No. 67, September, 17-23.
- Bogdanowicz, M., Scapolo, F., Leijten, J. & Burgelman, J-C., IPTS-ISTAG, EC: Luxembourg. www.cordis.lu/ist/istag
- Bohn, J., Coroamă V., Langheinrich, M., Mattern F. & Rohs M. 2003 Disappearing.
- Bohn, Jürgen, Coroamă Vlad, Langheinrich Marc, Mattern Friedemann, Rohs Michael, Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing° : web ref. <http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf>.
- Braun, Anette/Constantelou, Anastasia/Karounou, Vasilik/Ligtvoet, Andreas/Burgelman, Jean-Claude/Cabrera,
- Burgelman, J-C. 2001, How social dynamics influence information society technology: Lessons for innovation policy, pp. 215-222 in OECD, Social Science and Innovation, OECD: Paris.
- Cantoni Rejani 2004, 'Bodyarchitecture: the Evolution of Interface towards Ambient Intelligence', in (Riva 2004) part 3, chap. 11, pp. 213-219, http://www.vepsy.com/communication/book5/11_AMI_Cantoni.pdf [2 April 2005].
- CNIL (2006) , 27 rapport d'activité - http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-27erapport-2006.pdf
- Collste, G, Shahsavar, N, & Gill, H 1999, 'A Decision Support System for Diabetes Care: Ethical Aspects', *Methods of Information in Medicine*, vol. 38, no. 4-5, pp. 313-316.
- Computers Everywhere. Living in a World of Smart Everyday Objects, Paper for the EMTEL Conference, London 23-26 April 2003. www.inf.ethz.ch

- Conger, S. & Loch, KD 1995, 'Ethics and Computer Use', *Communications of the ACM*, vol. 38, no. 12, pp. 30-32.
- COST 219 terAccessibility for all to services and terminals for next generation networks, cost 219 ter, chapitre 4 Ambient Intelligence and implications for people with disabilities, web reference: http://www.tiresias.org/cost219ter/inclusive_future/ - pdf
- Crutzen, C.K.M. 2006, 'Ambient intelligence between heaven and hell; A transformative critical room?', in: Information society technology from a gender perspective - Epistemology, construction and empowerment, VSVerlag, as part of the series Interdisciplinary gender research, edited by the Centre for feminist Studies of the University of Bremen and the Centre of Womens and Gender Studies of the University of Oldenburg, 2006. web reference: <http://icommas.ou.nl/icm-cursus/Downloads/CSS-Crutzen-Intelligent-Ambience.pdf> .
- Culnan MJ 2000, Protecting privacy online: is self-regulation working? *J Public Policy Market* 19(1):20–26.
- Culnan MJ, Armstrong PK 1999, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organ Sci* 10(1):104–115.
- Dey, A. 2001, Understanding and using context. In: *Personal and Ubiquitous Computing* 5, Nr. 1, S. 4-7.
- Dey, A.; Mankoff, J.; Abowd, G.; Carter, S. 2002, Distributed mediation of ambiguous context in aware environments. In: *Proceedings of UIST 2002 Conference, User Interface Software & Technology*, Paris, 27-30 October 2002.
- Döring, S. A. & Goldie P., Principlism and the Applied Ethics of ECAs, ppt presentation: web ref. <http://emotion-research.net/ws/plenary2005/ethics.pdf>
- Dowling, C 2001, 'Intelligent Agents: Some Ethical Issues and Dilemmas', in *Proceedings of the 2nd Australian Institute of Computer Ethics Conference*, Canberra, Australia, pp. 28-32.
- ePOCH 2003, e-ID and the Information Society in Europe. White Paper. Website: http://www.eepoch.net/documents/public/WhitePapers/eepoch_white_paper.pdf.
- Eurobarometer 2002, 'Internet and the public at large', Flash Eurobarometer 125, Eos Gallup upon request of the EC, DG Information Society, July 2002, Brussels: European Commission.
- Final Report to the Commission on the Project Basic Ethical Principles in Bioethics and Biolaw, 1995-1998, coordinator Peter Kemp,
- Flichy, P. 1995, L'innovation technique. Récents développements en sciences sociales. Vers une nouvelle théorie de l'innovation, Paris: Editions La Découverte.
- Forty, A. 1986, *Objects of desire. Design and Society 1750-1980*, London: Thames & Hudson.
- Friedewald Michael, Wright David , Vildjiounaite Elenena (editors) (2005) Safeguards in a World of AmbientIntelligence (SWAMI): ScenarioAnalysis and Legal Framework – FirstResultsReport submitted to the participants of the first SWAMI expert workshop, held in Brussels, 1 June 2005.
- Friedewald, M., Costa, O., Punie, Y., Alahuhta, P., Heinonen, S. 2005, Perspective of ubiquitous computing in the home environment. *Telematics Information*, 22 (3),. 221-238.
- Goffman E 1961, *The presentation of self in everyday life*.Anchor-Doubleday, New York.
- Hamelink, Cees J. (2000) *The Ethics of Cyberspace*. Sage Publications.
- Hilty Lorenz M, Som Claudia, and Kohler Andreas 2004, Assessing the Human, Social, and Environmental Risks of Pervasive Computing, *Human and Ecological Risk Assessment*, 10:, 2004.
- International Review of Information ethics, Vol. 8 - December 2007, Ethical Challenges of Ubiquitous Computino, web ref. http://www.i-r-i-e.net/next_issue.htm
- Isaac, H. et Kalika, M., 2001, Organisation, nouvelles technologie et vie privée, *Revue Française de gestion*, Juillet- Aout, pp. 101-106.
- IST Advisory Group 2003, *Ambient Intelligence: From Vision to Reality. For participation – in society and business*. Luxembourg: Office for Official Publications of the European Communities. Website: <http://www.cordis.lu/ist/istag-reports.html>.
- IST Advisory Group; Ducatel, K.; Bogdanowicz, M. et al. 2001, *Scenarios for Ambient Intelligence in 2010*. EUR 19763 EN. Sevilla: EC-JRC, Institute for Prospective Technological Studies (IPTS). Website: <http://www.cordis.lu/ist/istag-reports.html>.
- ISTAG 2001, *Scenarios for Ambient Intelligence in 2010*, Edited by Ducatel, K..
- ITEA 2004, *ITEA Technology Roadmap for Software-Intensive Systems*, 2nd edition. Eindhoven: Information Technology for European Advancement (ITEA) Office Association. Website: www.itea-office.org.
- Johnson, D. G., 2001, *Computer Ethics*, 3rd. ed. Prentice Hall.

- L Venter, MS Olivier and JJ Britz, "Interactive to Proactive: Computer Ethics in the Past and the Future," in G Cöllste, SO Hansson, S Rogerson, and TW Bynum (eds) September 2005, *ETHICOMP 2005: Proceedings of the Eighth International Conference — Looking back to the future*, Linköping, Sweden, (Published electronically).
- Lessig L. 1999, *Code and Other Laws of Cyberspace*. Basic Books, New York NY, 1999.
- Lucas, R. 2001, 'Why Bother? Ethical Computers - That's Why!' in *Proceedings of the 2nd Australian Institute of Computer Ethics Conference*, Canberra, Australia, pp. 33-38.
- Lucky R. 1999, Everything will be connected to everything else. *Connections*. IEEE Spectrum, March 1999. Available at www.argreenhouse.com/papers/rlucky/spectrum/connect.shtm.
- Lyon D. 2006, 9/11, synopticon and scopophilia: Watching and being watched", in Kevin Haggerty and Richard Ericson (eds.), *The New Politics of Surveillance and Visibility*, Toronto: University of Toronto Press.
- Lyon, D. 1993, An electronic panopticon ? A sociological critique of surveillance theory, *Sociological Review*, Vol. 41, N.4, pp. 653-678.
- Manning Andre 2002, 'Research into women's impact on technology' in Philips News 2002.
- Mantovani Mario (draftman)) OPINION of the Committee on Employment and Social Affairs for the Committee on Industry, External Trade, Research and Energy on the proposal for a Council decision concerning the multiannual framework programme 2002-2006 of the European Community for research, technological development and demonstration activities aimed at contributing towards the creation of the European research area (COM(2001) 94 – C5-0087/2001 – 2001/0053(COD))
- Marcelino 2004, 'E-health in the Context of a European Ageing society', http://esto.jrc.es/detailshort.cfm?ID_report=1207 [30 december 2004].
- Marvin, C. 1988, *When Old Technologies were New. Thinking about electric communication in the late nineteenth century*. Oxford: Oxford University Press.
- Marx GT., 2001 Murky Conceptual Waters: The Public and the Private. *Ethics and Information Technology*, 3(3):157–169, July 2001.
- Mattern, F. 2003, Ubiquitous Computing: Scenarios for an informatized world, ETH Zurich, Paper to be published. <http://www.inf.ethz.ch/vs/publ/index.html>
- Meredith Rob and Arnott David 2003, On Ethics and Decision Support Systems Development, 7th Pacific Asia Conference on Information Systems, 10-13 July 2003, Adelaide, South Australia. web ref. http://e-learning.dmst.aueb.gr/mis/Cases/Nederlandse_Spoorwegen/Case/Training_Files/dss_ethics.pdf,
- Miles, I., Flanagan, K.. & Cox, D. 2002, Ubiquitous Computing: Toward understanding European Strengths and Weaknesses, European Science and Technology Observatory Report for IPTS, PREST: Manchester, March 2002.
- NRC/NAS 2001 - National Research Council; National Academy of Sciences: *Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers*. Washington, D.C.: National Academy Press.
- Orlikowski, W. J. 1991. Integrated information environment or matrix of control? The contradictory implications of information technology, *Accounting Management and Information Technology*, Vol. 1, N. 1, pp. 9-11.
- Parliament of Australia. October 2005, Research Note no. 14 2005–06 An overview of the effectiveness of closed circuit television (CCTV) surveillance, Nigel Brew Foreign Affairs, Defence and Trade Section 28.
- Philips News 2002 <http://www.newscenter.philips.com/about/news/section-13488/article-2235.html> - 2 April 2005.
- Philips Research 2003, '365 days - Ambient Intelligence research in HomeLab', www.research.philips.com/technologies/misc/homelab/downloads/homelab_365.pdf [2 April 2005].
- Pitkänen Olli and Marketta Niemelä, *Privacy and Data Protection in Emerging RFID-Applications*, pdf <http://www.rfidconvocation.eu/Presentations/14%20March/14%20March%20session%20convocation%20business/Privacy%20and%20Data%20Protection%20in%20Emerging%20RFID-Applications.pdf>
- Piva, S., Singh, R., Gandetto M. & Regazzoni C.S. 2005, 'A Context- based Ambient Intelligence Architecture', in Remagnino et al., 2005, pp. 65 – 66.
- PRIME Hansen, Marit and Henry Krasemann (eds.). 18 July 2005, *Privacy and Identity*

- Management for Europe – PRIME White Paper, Deliverable D 15.1.d.
- Punie, Yves. 2003, A social and technological view of Ambient Intelligence in Everyday Life: What bends the trend? IPTS EMTEL2 key deliverable Work Package 2 EU FP5 HPRN-CT-2000-00063 September 2003 Technical Report EUR 20975 EN
 - Quarterly, Vol. 38, N. 3, 1993, pp. 408-437.
 - Rhodes B, Minar N, Weaver J. 1999, Wearable Computing Meets Ubiquitous Computing – Reaping the Best of Both Worlds. In: Proceedings of the Third International Symposium on Wearable Computers (ISWC '99), San Francisco CA, October 1999, pp. 141–149.
 - Rieder, B. 2003, Agent technology and the delegation-paradigm in a networked society, Paper for the EMTEL Conference, London 23-26 April 2003. www.emtelconference.org
 - Riva G., Vatalaro F., Davide F. & Alcañiz M. (eds) 2004, 'Ambient Intelligence', IOS Press, 2004, <http://www.emergingcommunication.com/volume6.html> [2 April 2005].
 - Roszack, T. "Virtual Duck and Endangered Nightingale", In *PNLA Quarterly*, Vol. 59, no 1, Fall 1994, pp. 11-14.
 - Schmidt, Albrecht. 2004, 'Interactive Context-Aware Systems Interacting with Ambient Intelligence', in Riva et al. 2004, part 3, chap. 9, pp. 159-178.
 - Singer, I. 2001, Privacy and Human Nature. In: Ends and Means 5, No. 1. <http://www.abdn.ac.uk/philosophy/endsandmeans/vol5no1/singer.shtml>,
 - Smith HJ, Milberg SJ, Burke SJ. 1996, Information privacy.measuring individuals' concerns about organizational practices.MIS Quart 20(2):167–196.
 - Snapper, JW. 1998, 'Responsibility for Computer-Based Decisions in Health Care'. In *Ethics, Computing and Medicine: Informatics and the Transformation of Health Care*, ed. KW Goodman, Cambridge University Press, Cambridge, UK, pp. 43-56.
 - Spinello, R. 2000, Cyberethics: Morality and Law in Cyberspace. Jones and Bartlett.
 - Stahl, Bernd Carsten (2004): *Responsible Management of Information Systems*. Idea Group Publishing, Hershey PA.
 - SWAMI (Safeguards in a World of Ambient Intelligence) which aim to identify and analyse the social, economic, legal, technological and ethical issues related to identity, privacy and security in the forecasted but not yet deployed Ambient Intelligence (Aml) environment <http://swami.jrc.es/pages/index.htm>.
 - SWAMI, "Safeguards in a World of Ambient Intelligence (SWAMI): Pasi Ahonen et alii, final report, Deliverable D4 30 August 2006.
 - Tavani. H.T. 2004, Ethics and Technology: Ethical Issues in Information and Communication Technology. John Wiley and Sons.
 - United Nations 1948, The Universal Declaration of Human Rights *Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948* - <http://www.un.org/Overview/rights.html>
 - United Nations. 1966, International Covenant on Civil and Political Rights ().International Covenant on Civil and Political Rights Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 *entry into force* 23 March 1976, in accordance with Article 49 - http://www.unhchr.ch/html/menu3/b/a_ccpr.htm
 - Van den Hoven, J. 2007, "ICT and Value Sensitive Design" in Philippe Goujon, Sylvain Lavelle, Kai Kimpa, Veronique Laurent, The information society: Innovation, legitimacy, ethics and Democracy, ed. Springer, pp.67-72.
 - Warren S, Brandeis L. 1890, *The Right to Privacy*. Harvard Law Review, 4(1):193–220, December 1890
 - Weiser, M. (1991). "The computer for the 21 th century", draft for scientific American, Available at <http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>
 - Weiser, M. 1998, The invisible interface: increasing the power of the environment through calm technology. Keynote speech at CoBuld 98. Available at <http://www.darmstadt.gmd.de/CoBuld98/abstract/weiser.html>
 - Wood David Murakami and Ball Kirstie. 2006, A Report on the Surveillance Society For the Information Commissioner, by the Surveillance Studies network Public Discussion Document, September 2006.
 - Wright, D., 2005, The dark side of ambient intelligence, *Info*, Vol 7, No. 6, October, pp 33-51. www.emeraldinsight.com/info
 - Science and Society: Action Plan, EC, Com 2001, Brussels, 04.12.2001, 714 final

Copyright

Philippe Goujon © 2008 The author assigns the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

Ethics for IT: A short Weberian excursus

Darryl Coulthard

School of Information Systems

Deakin University

Melbourne, Australia

Email: darryl.coulthard@deakin.edu.au

The paper uses the famous conclusion of Max Weber's Protestant Ethic and the Spirit of Capitalism to open up the debate about ethics and the role of the professional. The paper identifies the key concerns of Weber in his conclusion and considers the implications for the development of IT ethics and the IT professional and the development of a professional response.

Keywords

Modernity, instrumental reason, professional ethics, social values.

INTRODUCTION

The Puritan wanted to work in a calling; we are forced to do so. For when asceticism was carried out of monastic cells into everyday life, and began to dominate worldly morality, it did its part in building the tremendous cosmos of the modern economic order. This order is now bound to the technical and economic conditions of machine production which today determine the lives of all the individuals who are born into this mechanism, not only those directly concerned with economic acquisition, with irresistible force. Perhaps it will determine them until the last ton of fossilized coal is burnt. In Baxter's view, the care for external goods should only lie on the shoulders of the "saint like a light cloak, which can be thrown aside at any moment." But fate decreed that the cloak should become an iron cage.

Since asceticism undertook to remodel the world and to work out its ideals in the world, material goods have gained an increasing and finally an inexorable power over the lives of men as at no previous period in history. Today the spirit of religious asceticism whether finally, who knows? has escaped from the cage. But victorious capitalism, since it rests on mechanical foundations, needs its support no longer. The rosy blush of its laughing heir, the Enlightenment, seems also to be irretrievably fading, and the idea of duty in one's calling prowls about in our lives like the ghost of dead religious beliefs. Where the fulfilment of the calling cannot directly be related to the highest spiritual and cultural values, or when, on the other hand, it need not be felt simply as economic compulsion, the individual generally abandons the attempt to justify it at all. In the field of its highest development, in the United States, the pursuit of wealth, stripped of its religious and ethical meaning, tends to become associated with purely mundane passions, which often actually give it the character of sport.

No one knows who will live in this cage in the future, or whether at the end of this tremendous development entirely new prophets will arise, or there will be a great rebirth of old ideas and ideals, or, if neither, mechanized petrification, embellished with a sort of convulsive self-importance. For of the last stage of this cultural development, it might well be truly said: "Specialists without spirit, sensualists without heart; this nullity imagines that it has attained a level of, civilization never before achieved" (Weber, 1958: 182).

This forms part of the famous conclusion by Max Weber in his groundbreaking and seminal work "The Protestant Ethic and the Spirit of Capitalism" which commenced publication in 1904. Certainly it is Weber, breaking free of cautious sociology, sounding something like an Old Testament prophet and the reference to the burning of fossilised coal is strangely contemporary but the reader may ask, what relevance does this have to the study of computer and professional ethics 100 years on? This paper

attempts to provide a reflection of this conclusion in the light of the development of ethics for computer, IT and IS professionals⁴⁴. The paper attempts to show that modern professional work entails a separation of ethics from efficiency and effectiveness concerns and that as a consequence ethics issues are marginalised and weakened by contrast to the centrality of efficiency and effectiveness. The paper is part of a larger project the ethics and the IT profession and this paper attempts to identify, using the quotation, the key problems and forces underpinning the difficulties facing the IT professional and the professional guilds in developing and maintaining an ethical stance in their work.

THE IRRESISTIBLE FORCE AND THE IRON CAGE

In simple and popular terms, “the irresistible force” that Weber refers to has been often been called “the march of progress”, the “march of reason” and those of a more radical persuasion the “march of capitalism”. For many they amount pretty much to the same thing and each of these expressions form part of the underlying assumptions of many IT professional. As scientists and scholars, the IT professions seek to discover and invent an contribute to the march of reason. As practitioners, IT professionals, the interventions they make into the world are typically intended to contribute to progress, and finally as business consultants and employees, there is a clear intention to contribute to capitalist enterprise.

As IT professionals concerned with ethics, we must look closely at the values and assumptions underpinning these commonplace views. As values they hold a particular stance towards human conduct and intervention and have important implications for how we act in our profession. To so do, we need to first discuss this ‘irresistible force’ in some detail. For Weber, this force is not any form of reason, but the development of what Weber termed ‘instrumental reason’ and for him and many who have variously taken his work seriously argue that the emergence of this type of reasoning underpins and for many, characterises, the modern age.

Instrumental reason is the separation of the means – how one gets to the end point most efficiently and effectively – from the end or goal of the means. That is, what one is trying to do is seen to be distinct from how one may try to do it. This distinction appears so commonplace and obvious that the modern reader is often blind to earlier forms of reasoning and consequently to the implication of this form reasons for ethics, professions and society at large. Instrumental reasoning can be contrasted with ‘value rationality’ where the end goals are not split from efficiency and effectiveness concerns and form part of the reasoning process.

Weber developed his theory of bureaucracy upon instrumental rationality. Weber’s concern was to identify what was the most ‘rational’ – ie effective and efficient organisational structure. Information Systems in particular uses instrumental reasoning to identify the most efficient and effective information system to achieve the ends of the organisation. The purpose of the bureaucratic manager, the IT expert is to deploy their knowledge of a given situation to identify and implement a solution or practical outcome that meets the needs and goals of the organisation or client.

The key point for this discussion is that the IT expert is not concerned, *at least in his or her capacity as an expert*, with the ends, themselves. The means are amenable to reason and science but the ends are external to the exercise. From this instrumental perspective (one that MacIntyre (1981) terms ‘emotivism’) values are not amenable to reason and are in this sense arbitrary and irrational. The ends are subject to the intentions of governments, shareholders or those who speak for them. Values, laws and social customs may form an enveloping constraint on the efficiency and effectiveness of a solution but values themselves remain external to the task of the expert.

The melancholy observation of Weber’s that ‘reason’ had been reduced and narrowed to servicing the economic machine is but one aspect. That this is ‘irresistible’ with no obvious alternative adds to the melancholia. It is irresistible in the sense that it is almost impossible to think of an alternative mode of reasoning to the current situation where ethics – the discussion of ends – is external to the enterprise.

⁴⁴ For brevity, I will term all computer, IT and IS professionals, scientists, engineers and academics in the following as “IT professionals”

The practical implication is that for the expert, values are not his or her concern, as an expert. He or she is not qualified, as an expert, to judge or comment on the ethics of the ends. They are structurally and practically separated from such ethics. Ethics or goals are a matter for the shareholders or whoever is paying for the service. This, as Bauman (1989) has persuasively argued is part of the fundamental mechanism that produced the horrors of the Nazi genocide. The experts, professionals, soldiers and managers undertook their tasks with lesser or greater zealotry or with lesser or greater misgivings. Engineers solved technical problems of horrible genesis and designed more and more effective genocidal machines that their masters lawfully asked them to produce. Were IT as central to the economy and administration of the Third Reich there seems little doubt that it would have been applied with frightening efficiency and effectiveness. Indeed, there is some evidence that IT was used by the Nazis to more easily identify Jews and other groups of interest (cf Dillard, 2003).

The business of ends is not the business of the expert qua expert. It may be suggested at this point that such ends is the business of the professional. The IT professional as opposed to the expert does, or at least should, consider the ends of his or her work. Whether or not IT professionals have the ability and willingness to consider ends and to what degree, is an empirical question and is one that needs to be examined. It seems unlikely that IT professionals are well prepared to take on the ethics of their actions of, say, issues of privacy, copyright protection, workforce deskilling and so on. It is clear that the discussion of ends is in practice peripheral or marginal to their expertise.

IT professionals at the Australian Wheat Board may have been aware or might have made it their duty to be aware of the illegal and unethical dealings of the AWB. IT professionals in the US would almost certainly have known of the dealings of the Enron. These are difficult and complex matters and it appears overly moralistic and harsh to blame these professionals for failing in moral courage and conviction to blow the whistle. The uncoupling of means and ends undermines the role of the professional and advances the technical prowess of the expert.

IT is part of the project of modernity – the drive for efficiency and effectiveness - finding the best route to a given end that an organisation can take. The IT expert (as an ideal type) is amoral at the service of the organisation and within the bounds of the law. The IT expert is not really paid or recruited for anything more. To this extent the IT professional is an anachronism and a hindrance to industry. This is the IT professionals 'iron cage' where it becomes almost impossible to argue against a given end as the professional is not directly responsible for that end. It would be difficult, say to argue against providing poor and unreliable software that may well be the best commercial solution, one that gives the shareholders the maximum return. A cost benefit analysis may demonstrate this. The IT professional may well shrug his or her shoulders in face of this argument – they aren't responsible for the decision. It may be one thing to argue against something that is illegal but another to argue against what may well be good business practice.

THE ROSY BLUSH OF ITS LAUGHING HEIR, THE ENLIGHTENMENT, SEEMS ALSO TO BE IRRETRIEVABLY FADING

This is an extraordinarily prescient statement from Weber, written as it was at the apogee of the modern age, some ten years prior to the first disaster of the First World War, where the mechanised age marched into mud and blood. It is a postmodern statement. In one sense his view is incorrect, the 20th century, the big ideas of the Enlightenment (cf. Bauman, 1989) went off with a bang – Nazism and Stalinism, rather than a whimper. However, taking a long view there is indeed some argument to suggest that our ideas are indeed exhausted and our focus on the "purely mundane passions" of capital accumulation and consumerism (Ritzer, 2004).

Turning this view onto the IT profession, there is some argument to suggest that most of our efforts are on the 'purely mundane passions'. For all the professional talk of an information revolution, our ideas seem somewhat stuck on developing more efficient information systems, eCRM, iPods and so on. There appear to be few big ideas outside of commercial success or increased business efficiency. Few IT professionals are leading or substantially contributing to the progressive and regressive effects of IT and how IT can aid social and environmental reform.

SPECIALISTS WITHOUT SPIRIT, SENSUALISTS WITHOUT HEART

A specialist without spirit, a sensualist without heart is the expert. What appears lacking is the notion of vocation, of calling. A casual inspection of the typical job description for any professional job will list a range of skills and attributes. In general terms, the successful applicant will be able to address or demonstrate the following: demonstrate the prerequisite technical skills, capabilities and qualifications, demonstrate project and people management skills required the level of position and provide examples of quality work and work of complexity and significance. The applicant *inter alia* may also directly address their interpersonal and communication skills including their ability to work in teams and others.

The picture that emerges from the job description is one of the professional who has the expertise to do the job and preferably excel in the technical and managerial challenges placed before him or her. It also means that the professional has in the past worked well with organisations and with those people in the organisation: that the professional can work well within the social and organisational constraints of the modern organisation and finally they are more or less personable and can work well with others.

The ability to work well with others usually tails the key selection criteria, partly because it is difficult to demonstrate directly other than via referees, partly because there is the assumption that those who don't work well with others typically don't do that well within organisations unless the job is especially esoteric or technical and partly that those who cannot work that well have been weeded out in previous jobs.

Finally, there may be some prescription, most commonly in NGO and government organisations that the person can work within the values of the organisation. This is only rarely addressed in the selection criteria and even more rarely tested or examined closely in interview. The assumption here seems to be that the values of the organisation tend to be self selecting. By all these criteria, people, not surprisingly and unremarkably, are selected for their efficiencies and effectiveness, not their values and their willingness to stand by them.

Current ethical theories place the individual in a precarious position. On the one hand, the self is the arbiter of all moral values but on the other the self works in organisations where values are taken as given (MacIntyre, 1981:33). The individual is very much caught in a 'take it or leave it' bind. The self historically has been a locus of social relations; one is what one's role and place within the community. There is ample evidence now to suggest that at least in the West, our identity is no longer to be found in these collective, social relations (Beck, 1992; Sennett, 1998; Putnam, 2000). To this extent, our ability to make moral choices, working with others to develop a position is far weaker. This is well illustrated in Hariman and Lucaites (2007) work on iconic photographs when they show the movement from the collective effort such as raising the US Flag on Iwo Jima to that of the lone man facing the tanks in Tiananmen Square. It would seem as if we have now God like responsibilities for moral decision but little means to decide or to act collectively on our moral responsibility. We may exhort ourselves to be more ethical but there may be something wrong with our selves and our ethics.

While Weber appears to be speaking of the stripping away of value from the expert in his statement, we can glimpse too the emergence of a fragile self, trapped in the mechanisms and procedures of the organisation: Weber's iron cage.

NEW PROPHETS: HOW SHOULD WE THINK ABOUT ETHICS?

Weber ends pessimistically: he had no answer. Postmodernism is itself an expression of this view. Like Chou En Lai's response to the question of the effect of the French Revolution, whether there are new prophets or the refurbishment of old ideas, it is too "early to tell". Nevertheless, there are changes, and there has indeed been the re-emergence of the old ideas of Aristotelian ethics through work of MacIntyre (1981), new ideas with the work of Bauman (1993) and also the emergence of a critical business ethics informed by social and organisational critique and recent ethical theory (Jones, Parker and ten Bos (2005).

MacIntyre argues that the Enlightenment, following its general scientific critique of Aristotle, jettisoned Aristotle's teleological scheme while retaining its ethical precepts. Aristotle's teleological scheme as it applied to morality was 'man-as-he-happens-to-be', 'man-as-he-could-be-if-he-realised his-essential-nature' and the application of practical reason and the virtues aimed at assisting man's realisation of his essential nature. The Enlightenment stripped the guiding principles – the practical manual for living the good life – and elevated it to law-like, external forces on everyday conduct. Human beings were no longer conceived of as human 'becomings' or 'works-in-progress' that were using ethical precepts as guides but as finished, autonomous selves acting independently in the world and constrained by moral forces. Again we see here in the Enlightenment an overweening view of the self divorced from its social location.

The alternative view is to consider morality as a process of becoming which is grounded in the conduct of everyday life and engagement in social life and practice and where the development of moral character takes precedence over the following of rules. MacIntyre suggests the redevelopment of virtue ethics. This moves morality from the realm of society and of rules and regulations to that of everyday practices and concerns.

Bauman (1993) provides a complementary view to MacIntyre. Bauman's (1989, 1993) essential insight, following his work on the Holocaust, is the corrupting influence of social institutions and that by following ethical, laws, rules or guidelines and that by following such rules 'we put morality to sleep'. This view echoes MacIntyre's view that ethics and the self as unfinished process of becoming.

Finally, Coulthard (2005) and Jones *et al* (2005) provide a critique of current textbooks and teaching of business and IT ethics. In particular, they note that most professional and business textbooks severely circumscribe ethics to a narrow area of philosophy and professional practice. They argue that most textbooks confine ethical theory to the Enlightenment theories of the 18th and 19th Century. Ethical issues, they argue, are further limited to particular issues and an individualist approach to ethics is encouraged. However, many ethical problems and dilemmas are social and political problems that cannot simply be resolved by our individual action. As with MacIntyre and Bauman, ethics is not a set of clearly defined problems facing an individual but a particular perspective and way of living the good life.

The key issues facing the development of IT ethics must involve the profession wrestling with the concerns of modernity and recognising the iron cage of which it is part. It must, as Jones *et al* (2005) suggest, broaden its concerns from a focus of the individualistic ethics to one that encompasses a greater understanding of the social, organisational and political context in which ethics operate and choices are taken. It must, to use a recent expression, embed the ethical in all aspects of professional and social life (McDonald, 2007).

REFERENCES

- Bauman, Z. (1989). *Modernity and the Holocaust*, Cambridge: Polity Press.
- Bauman, Z. (1993). *Postmodern Ethics*, Oxford, UK ; Cambridge, Mass.: Blackwell.
- Beck, U. (1992). *Risk Society: Towards a new modernity*, London: Sage.
- Coulthard, D. (2005) The morality of the everyday: An initial step towards a research strategy, *Proceedings of APROS 11, Asia-Pacific Researchers in Organization Studies, 11th International Colloquium*, 4-7 December 2005, Melbourne
- Dillard, J. F. (2003). *Professional Services, IBM, and the Holocaust*, *Journal of Information Systems*, 17(2), 1-16.
- Giddens, A. (1991). *Modernity and Self-identity: Self and society in the late modern age*, Cambridge: Polity.
- Jones, C., Parker, M., & ten Bos, R. (2005). *For Business Ethics: A critical text*, (1st ed.). New York, N.Y.: Routledge.
- Hariman, R., & Lucaites, J. L. (2007). *No caption needed: iconic photographs, public culture, and liberal democracy*, Chicago: University of Chicago Press.

- MacIntyre, A. (1981). *After Virtue: A study in moral theory*, Notre Dame, Ind.: University of Notre Dame Press.
- McDonald, C. (2007). Embedding Ethics in Systems Development. *Proceedings of ACIS 2007 18th Australasian Conference on Information Systems Embedding Ethics in Systems Development*, 5-7 Dec 2007, Toowoomba.
- Putnam, R. D. (2000). *Bowling Alone: The collapse and revival of American community*, New York: Simon & Schuster.
- Ritzer, G. (2004). *The McDonaldization of Society*, (Rev. new century ed.). Thousand Oaks, Calif.: Pine Forge Press.
- Sennett, R. (1998). *The Corrosion of Character: The personal consequences of work in the new capitalism*, (1st ed.). New York: Norton.
- Weber, M. (1958). *The Protestant Ethic and the Spirit of Capitalism*, New York: Scribner and Sons.

COPYRIGHT

Darryl Coulthard ©2008 The author(s) assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

The Ethics of Information Operations

William Hutchinson

School of Computer and Information Science

Edith Cowan University

Perth, Australia

Email: w.hutchinson@ecu.edu.au

Abstract

The underlying objective of information operations (information warfare) is to achieve 'information superiority' over all perceived opponents. Achieving this can involve such activities as manipulating digital systems, deception, surveillance, propaganda, influence, psychological operations and data hiding. This paper will examine the positive and negative ethical implications of such practices. It posits that the end result and motives for these activities are paramount in determining the ethical outcomes. However, it also recognizes that 'the end justifies the means' has some dangerous implications.

Keywords

Information operations, information warfare, just war, ethics, influence, psychological operations, propaganda.

INTRODUCTION

The concept of 'information operations' (or its sub-set, information warfare) was developed from a series of ideas in the American military. Initially intended to exploit the new capabilities of integrated computer networks for command and control and intelligence, it evolved into a more sophisticated set of concepts and practices that reflected the developing Information Age. Its evolution moved from the technocentric ideas of computer warfare to include many others of a more psychological nature. The stated aim of information operations activities is to create *information superiority* and to deny such an advantage in an opponent (JP 3-13 2006). This superiority is necessary to dominate the *infosphere* that is, the area of operations that involves the communication and interpretation of data (Hall 2003). By this definition, it has conflict as its *raison d'être*, because of this its application to the business community is normal where the term *conflict* is replaced by *competition*. In achieving information superiority, a number of techniques can be used including, but not restricted to, attacking and defending computer networks, deception, propaganda, surveillance, censorship, and psychological operations. Its objective is to dominate the infosphere using any technique that will gain, deprive or manipulate information for advantage. This has obvious ethical implications. Using the concept of *just war* as a framework, this paper examines these ethical issues.

'JUST WAR'

In conflict there are two basic ethical issues when considering the 'justness' of war. They are: the reasons for the *just war* (*Jus ad Bellum*), and the way the *just war* is fought (*Jus in Bello*). The accepted reasons for a just war include: right purpose (a justifiable reason), a duly constituted authority (that is, not an individual), and last resort (that is other avenues have been followed before the conflict). The ethical concepts concerned with the just 'means' of fighting a war include: non-combatant immunity (that is, innocents should not suffer), proportionality (the methods should be proportional to the threat, and also to the strength of the relative strength of the enemy), and more good than harm should come of the war (this means that the use of force should result in more good than harm). (Arquilla 1999, pp. 381-383).

Information operations can have offensive and defensive modes. Defensive postures can often be justified ethically and consist of conventional information security and counter-intelligence. These are practiced to preserve the confidentiality and integrity of the information systems and the data stored

and transmitted. Whilst, there could potentially be problems with the concepts of secrecy, the right to preserve the data owned by an organisation is rarely questioned. However, the more offensive tactics use in information operations brings it into conflict with ethical considerations. It is these considerations that will be covered below. However, it must be stated that in terms of violent conflict, the main aim of information operations is to minimise collateral damage and to ensure that the violence is restricted to the real battlefield. Thus, ensuring the safety of one's own side and minimising the length of the aggression. In fact, the major aim of psychological warfare is to avoid violence altogether (MacDonald, 2007). However, there is a major dilemma: can the ends justify the means? As the various aspects of information operations are numerous, this paper will discuss two of them from the opposite ends of the tactical spectrum: the techno-centric and the psychological.

DIGITAL CONFLICT

The concept of information operations was borne with the development of digital computers and networks. (Initially, it was known as 'information warfare' but this term is now restricted to information operations during periods of overt conflict.) In conflict, this technology gave an advantage in processing power and, with appropriate sensors, the ability to collect and manipulate intelligence at speed. In fact this developed into the concept of 'network centric warfare' (Alberts *et al*, 1999). Simultaneously with the advent of this technology came the tactics to protect this asset as well as disrupting or destroying an opponent's ability to do the same. Digital operations might involve bringing a system down, destroying data, inserting erroneous data, extracting data for advantage, and inserting malicious code for various reasons.

Jus ad bellum

In this case the concepts of right purpose and a duly constituted authority must still be upheld. It is problematic for terrorists or criminals to carry out these activities as some terrorist groups would argue that that are a duly constituted authority within their own support base, or perhaps to reverse it, would claim that their enemy is not, regardless if it was a government or not. However, these arguments are true for all type of war-fighting. In terms of 'last resort', information operations tend to be practiced before any open conflict starts. Intelligence gathering, degrading opponent's systems, and inserting malicious code occurs before hostilities are open. This is even more pronounced in psychological operations examined below. If a Hobbesian view of conflict taken that humans will use every means with force behind it to get what they desire (Donnelly 2005) then these precautions are necessary as humans and nations are constantly in a state of conflict. If this realist stance is taken then it would be totally irresponsible for those with the remit for national security not to take these precautions. Libicki (2007) argues that the application of these 'digital' precautions on an enemy degrade the ability to actually wage war, and thus, might avoid it. Of course, this must be coupled with the concept of right purpose to be ethical.

Jus in bello

The use of attack strategies on digital systems is more problematic as non-combatants are often not immune, many of the tactics in computer based warfare involves the degradation of systems that provide services such as power or emergency services. Thus, those that suffer could be only indirectly involved such as hospital patients. Another major target is often communication networks which are often run over public systems. So in an ethical sense, attacks on digital systems can be as random in consequence as carpet bombing if not so physically destructive. Because of the redundancies in networks, it is necessary to take the whole network down.

As one of the major aims of information operations is to stop enemies from being able to command and control their resources, this type of attack tends to be out of proportion to the threat as it is a deterrent to further violence. Hence, all media outlets are brought down, the means of communications are degraded and power sources are neutralised. The ability to carry out these operations tends to lie with powerful nations, notably the United States. Hence the ability of the 'enemy' nations, for instance, Serbia in the 1990s, to have comparable abilities is not present. In a sense, this type of attack on a less technically advanced nation goes against the spirit of non-proportionality. However, the adherents of information operations would claim that 'more good than harm' would have come from this sort of attack as it targeted equipment rather than people directly, and also, that it shortened the length of the conflict. It is ironic that technology in the form of the Internet allowed the Serbians to run a very successful propaganda campaigns (Hentea, 2006).

Strangely, NATO command did not isolate Serbia from the Internet which it was in the position to do so. It is always a good idea to leave open communication channels if for no other reason than allow propaganda from both sides to flow. Nevertheless, Rowe (2007) indicated that some reckless use of digital attack methods amount to war crimes.

COGNITIVE CONFLICT

Whilst much is made of information technology in the contemporary world, it is the use of the data obtained from them that is the greatest consequence. Thus, the distribution and context of data presented can influence decisions that are made (and can be made because of the available data) as well as the attitude of the recipient. In terms of a conflict, psychological operations are those that use influence techniques as well as violence to encourage the enemy to surrender; it has one end: to stop the enemy from fighting rather than win their 'hearts and minds'. Propaganda is the name given to techniques that attempt to influence people in both the short and long term. It is often used to give a specific context for action. Figure 1 summarises the intention of various types of influence operations. Psychological operations are used to enforce compliance whilst propaganda tends to be used to produce conformity and assist conversion. Education and other socialisation processes are needed for long term conversion to a way of thinking.

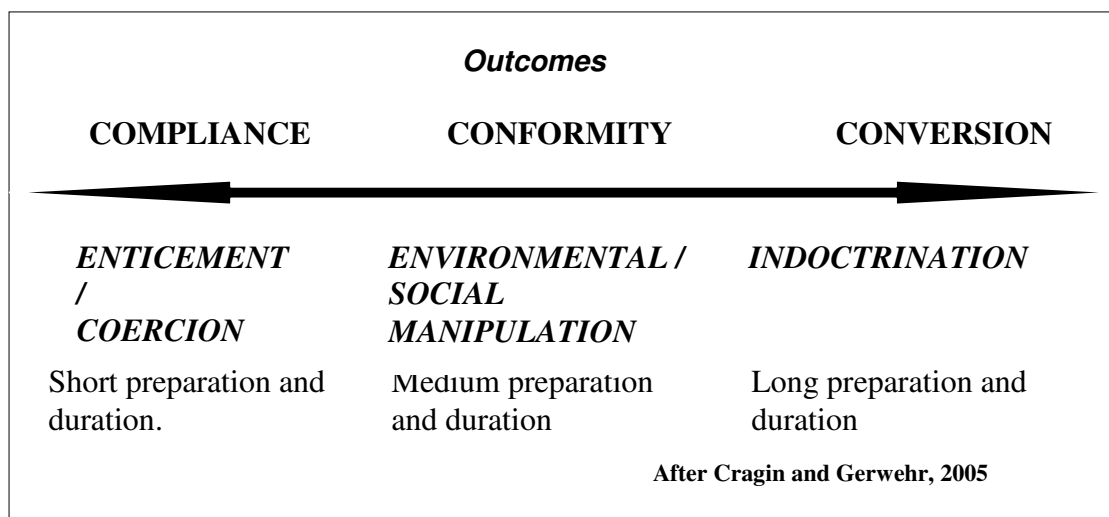


Figure 1: Elements of Strategic Influence Operations

Indoctrination has the greatest overall impact to the human whilst coercion, seemingly the most unethical, has ironically the shortest impact. Along with this comes the practice of deception which is seemingly an unethical practice, however, its adherents would claim that its practice will save lives if used in certain circumstances (Bennet. & Waltz, 2007).

Jus ad bellum

As with the technological aspects of information warfare above; tactics in the cognitive realm assume that the concepts of right purpose and a duly constituted authority must still be upheld to remain both ethical and legal. However, in terms of 'last resort', cognitive tactics are used both in period of conflict and peace. It can be argued that this can both avoid and encourage conflict.

Jus in bello

In terms of proportionality and non-combatant immunity these techniques are designed to cover everyone on the side of the enemy. In some situations, enemy commanders can be targeted for psychological operations as happened in 2003 Iraq war but generally whole populations both combatant and non-combatants are the receivers of the messages. In this war, control over the 'ideas' was manipulated by the coalition governments to an extent which belied the use of 'embedded'

journalists. Control of the major messages sent out from the conflict was dominated by compliant media companies. The development of 'militainment' started during the Gulf war of 1991 was expanded during the Iraq War, and produces a number of ethical problems. The military and entertainment nexus was not exactly new but now war was drama with its own suspense and excitement (Schwartz, 2004). However, rarely were shattered bodies shown. Another dimension was what Adie (2004) calls the depiction of weapons as 'sexy' that is, the visual spectacular of explosions on the horizon after the rocket or cruise missile is launched gives immense gratification although the consequences, such as mutilated bodies, are not shown. Of course, in war morale boosting propaganda has been used for a long time, as has deception; it is just that modern technologies make them so much more convincing and immediate. A classic propaganda deception was that of the rescue of Jessica Lynch. Key symbols were used with the televising of the rescue. Brown (2004) says these key symbols were used to "make grown men and women kill" (p.81) and the rescue of Lynch was "literally pregnant with meaning among the universe of symbols that are part of a grand narrative". The 'official' rescue of this "plucky, white American soldier" fought off the "degenerate, blood drinking, cowardly, sub-human Iraqis" (p.82) after emptying her magazine into them and being stabbed and overwhelmed. Again the vilification and stereotyping of the enemy is not new but the power and universality of modern technologies mean they have immediate effect.

Marlin (2002) posits that there should be a number of ethical constraints on propaganda;

- If propaganda provokes some form of action then it must be evaluated by those actions and the motivations for those actions, for example, greed;
- Even if the outcome sought is good then the tactics used must not go beyond certain limits. So for instance, even in conflict racism or stereotypes should not be used if this goes beyond the conflict itself; and
- The use of emotional levers should not conflict with the morality of the outcome sought.

In other words, to maintain an ethical campaign constraint must be practice at the expense of short term gain and the end should be worthy of the tactics used. It is this relative nature of ethics in information operations that seems to take precedence.

CONCLUSION

The objective of information operations is to avoid aggressive actions or if they do occur to ensure a short period of conflict. It tends to target equipment, software, and the attitudes and understanding of humans without physically damaging them. Whilst this in itself surfaces other ethical issues such the legitimacy of deception, its intent is to minimise overall physical harm. So, even when the use of surveillance and digital systems are used to guide weapons to a 'certain' hit, this can be justified as it minimises collateral damage and ultimately shortens the conflict. Whilst the ethics of war itself are problematic, this paper argues that information operations have an ethical basis within the context of war. This argument must be supplemented with the need for a just war as defined above and restraint in the tactics used. Hence, although many of the tactics used in information operations would be considered unethical in themselves, if they are used in certain contexts might be the most ethical option.

Information operations raise a number of issues that need to be investigated. Whilst the practice of such things as deception, data manipulation, surveillance and physically attacking communications is not questioned during overt war conditions (although there are still rules), their practice during periods of peace, or 'near' war (which the followers of Hobbes or Machiavelli would say is the perpetual situation) is questionable. The practice of information operations has as its *modus operandi*, the need to dominate and control data and information whenever and whatever the situation. Thus, such practices as long term influence operations need to be performed whether there is overt conflict or not. The ethics and legality of these situations are still unclear and need to be examined further.

REFERENCES

- Adie, K. 2004. *Press Club*, Australian Broadcasting Corporation, 55 mins, 13.00hr, 22 December 2004, television.
- Alberts, D.S., Garstka, J.J., Stein, F.P. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority – 2nd Edition*, CCRP Publications, Vienna, VA.

- Arquilla, J. 1999. *Strategic Appraisal: The Changing Role of Information in Warfare*, RAND Institute, Santa Monica.
- Bennett, M., Waltz, E. 2007. *Counter-deception: Principles and Applications for National Security*, Artech House, Norwood, MA.
- Brown, C.W. 2004. 'Where's Jessica? Myth, Nation, and the War in America's Heartland', *Social Analysis*, vol. 48. no.1. pp. 81-85.
- Cragin, K., Gerwehr, S. 2005. *Dissuading Terror: Strategic Influence and the Struggle against Terrorism*, RAND, Santa Monica.
- Donnelly, J. 2005. 'Realism', in: S.Burchill and A.L. Linlaker (eds) *Theories of international relations*, 3rd Edition, Palgrave MacMillan, Basingstoke, pp.29-54.
- Hall, W.M. 2003. *Stray Voltage*, Naval Institute Press, Annapolis, Maryland.
- Hentea, C. 2006. *Balkan Propaganda Wars*. The Scarecrow Press, Oxford.
- JP 3-13. 2006. *Joint Publication 3-13 Information Operations*, Joint Chiefs of Staff, Washington, Available online: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf
- Libicki, M.C. 2007. *Conquest of Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York.
- Macdonald, S. 2007. *Propaganda and Information Warfare in the Twenty First Century*, Routledge, Abington.
- Marlin, R. 2002. *Propaganda & the Ethics of Persuasion*, Broadview Press, Peterborough, Ontario.
- Rowe, N.C. 2007. 'War Crimes from Cyber-weapons', *Journal of Information Warfare*, vol.6, no.3, pp. 15-25.
- Schwartz, J. 2004. 'A Cast of Thousands: The Media and the Staging of Gulf War' Two, *Australian Screen Education*, vol. 22, pp. 52-57.

COPYRIGHT

W.Hutchinson ©2008 The author assigns the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

Ambient technology: Reconsidering informed consent

Penny Duquenoy

School of Computing Science, Middlesex University, London, UK,
p.duquenoy@mdx.ac.uk

Oliver K. Burmeister

School of Computing and Mathematics, and Centre for Applied
Charles Sturt University, Australia
oburmeister@csu.edu.au

ABSTRACT

New forms of ambient technology are emerging. Human computer interaction continues, but with an at time invisible interface. Agents monitor seniors in their homes to ensure medical doses are taken in timely and correct fashion. Testing the usability of such technology raises numerous ethical concerns, particularly to do with enabling participants in such testing make informed decisions. Current principles of informed consent, as used in the human computer interaction profession, may be inadequate to the task ahead.

Keywords

Informed consent, transparency, seniors, medical technology.

INTRODUCTION

Human Computer Interaction (HCI) is facing new challenges. The context in which HCI work and research takes place today has to cater to ever increasing diversity of technology, especially in the area of medical technology. The challenges of ubiquity, pervasiveness and ambience all bring new challenges to the way in which research and practice involving human participants takes place. It can be envisaged that in a context of an ambient environment, where the technology disappears, carrying out informed consent procedures using traditional approaches, will no longer be appropriate. Yet this should not mean that one discards considerations of risks to the human participants in this work. These new technologies raise difficulties with 'informed consent', in terms of compliance and other issues. How will HCI address these issues?

Whilst not writing in an era of transparent and disappearing technology, Moor (1985) drew attention to the ethical aspects of computer technology given by its social impact, and characteristics of logical malleability and invisibility. The challenges posed by invisibility, for Moor, were the potential for invisible abuse, the invisible values that are embedded in programs, and the capacity for complex calculations that are beyond human understanding. To this list we can now add the invisible computer which removes another layer of observation.

The paper begins by placing 'informed consent' in its current context in HCI. A review of the literature shows there are 10 principles relating to informed consent, at least 8 of which are cited frequently enough to lead one to assume these are generally accepted in the HCI community. The paper continues by detailing two case studies that illustrate why informed consent issues are important in HCI. Next the challenges to HCI of disappearing technologies are discussed with, with reference to the same case studies, illustrating the possibilities for invisible abuse that can arise, without due consideration of informed consent issues. The paper concludes by recommending that participants deserve to be given a broad context of use and understanding, especially given the new contexts and appearance (or disappearance) of these technologies.

INFORMED CONSENT

Existing literature on 'informed consent' in HCI focuses on the traditional means of selecting representative samples from the potential user base to participate in assessments of product usability at a single, controllable location. Writing in the context of usability testing, Dumas and Redish (1999)

said that the focus of usability testing on users extends to issues such as enabling users to be productive with software products, helping them accomplish tasks they need or want to engage in easily and quickly. In terms of engineering products that are usable, they argue that early and continuous focus on usability will lead to functionality that will be used, identifying needed changes before making such changes becomes too expensive, facilitation of the development of documentation and training, and reduction in the amount of product maintenance that will be required.

Dumas and Redish (1999) give multiple examples of the usability laboratories (labs) set up for traditional usability situations. In large organisations such labs can involve multiple testing suites, each equipped with an observation room and an executive viewing area. Each test room would typically have three or more cameras, with data-logging facilities in the observation room. Some labs are equipped with video conferencing facilities that connect to large rooms from which an entire development team, management and clients can observe the test.

Out of respect for participants and also to ensure unbiased results people participating in a usability test are informed about what will happen during the test, how they will be affected and what their rights are during and after the test. Informed consent policies exist to safeguard both the participant and the organisation conducting the test.

The Legal Argument For Informed Consent

Informed consent is part of the larger issue of ethical experimentation. In most western countries implementing policies regarding informed consent is a legal requirement. Dumas and Redish (1999, pp204-205) writing in the context of the American legal system, cite the Notice of Proposed Rulemaking in the Federal Register, 1988, Vol. 53, No. 218 pp 45661-45682, on the treatment of human participants, as the grounds for requiring a formal consent procedure prior to any usability test in that country (at least for all usability testing that is federally funded). Similarly the Australian 'National Statement on Ethical Conduct in Research Involving Humans' (Commonwealth of Australia, 1999), affirms the principle of respect for persons. This principle requires that participants be treated with respect as autonomous agents and that participants with diminished autonomy (such as the young and the physically and intellectually impaired) are entitled to special protection. In the UK vulnerable groups are described as: children and young people, those with a learning disability or cognitive impairment, or individuals in a dependent or unequal relationship (ESRC, 2007). The informed consent process ensures the risks and benefits of the test are disclosed to participants or their guardian before the investigation can proceed.

In addition to legal requirements by governments, there are also professional society stipulations that require respect for participants in testing software products (ACS, 2007; APA, 1997; BCS, 2007). Dumas and Redish (1999) argue that even if there is no threat of possible legal action against a company engaging in usability testing, formal procedures for informed consent should still be followed. They reason that this reduces an organization's vulnerability to appearing negligent in regards to proper treatment of human participants in those tests.

Miller (1998) writing in the context of software engineering states that informed consent is complete when the form has been signed. However, in usability testing informed consent is more than the legal requirement of a form that must be signed. As in medicine (Mackay, 1991), in usability engineering informed consent is an attitude that begins when the facilitator greets the participant and continues until the participant leaves. Medical practitioners are to inform patients to the extent of what patients might reasonably want to know about a therapy the practitioner is recommending. Mackay's (1991) review of this area showed that poor communication was frequently the cause of patients refusing treatment. In the context of informed consent in usability testing, this supports the view that by building rapport and supplying information to participants, one is more likely to get their cooperation to proceed with the test.

WHY IS INFORMED CONSENT IMPORTANT?

Policies regarding informed consent in HCI are developed by organisations on the basis of generally agreed principles concerning the treatment of human participants. Seven of the principles that follow are derived from the related discussion in Dumas and Redish (1999, pp205-208), though in their presentation they only view principles P2, P3 and P4 as principles of informed consent. They see their other principles as part of the wider issues involved in the legal requirements that need to be met prior to a usability test. One of the additional principles was suggested by Sanderson (2000) in a review of

Dumas and Redish on usability testing. The last two principles were suggested by Burmeister (2001) for the context of remote usability testing.

P1 Minimal risk

Usability testing should not expose participants to more than minimal risk. Though it is unlikely that a usability test will expose participants to physical harm, psychological or sociological risks do arise. If it is not possible to abide by the principle of minimal risk, then the usability engineer should endeavour to eliminate the risk or consider not doing the test. If the test needs to go ahead despite the risk then there are well established policies put out by many of the psychological societies that can serve as a basis for ensuring the protection of the rights of participants (APA, 1997).

Dumas and Redish (1999) citing the Federal Register state that minimal risk means that “the probability and magnitude of harm or discomfort anticipated in the test are not greater, in and of themselves, than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.” (1999, p205) Similarly the Australian ‘National Statement on Ethical Conduct in Research Involving Humans’ (Commonwealth of Australia, 1999), has a principle of beneficence, which involves maximizing the possible benefits and good for the subject, while minimizing the amount of possible risks and harm, as does the Economic and Social Research Council’s research ethics framework (UK) (ESRC, 2007).

P2 Information

Informed consent implies information is supplied to participants. Information to include suggested by Dumas and Redish (1999) can be summarized as: the procedures you will follow; the purpose of the test; any risks to the participant; the opportunity to ask questions; and, the opportunity to withdraw at any time. This principle of ‘information’ might be extended to what participants are told about the test when they are solicited to participate. They could for instance be sent a letter detailing in advance what will be recorded and what they will be doing.

P3 Comprehension

The facilitator needs to ensure that each participant understands what is involved in the test. This must be done in a manner that is clear. It must also be done so as to completely cover the information on the form. The procedure for obtaining consent should not be rushed, nor made to seem unimportant. The procedure is about the participant making an informed choice to proceed with the test and therefore they need to be allowed opportunity for questions. In a remote test this might be managed with a facilitator on site with the participant. Clearly one possible outcome of applying this principle is that the person involved may choose not to participate. However, not to permit such opportunities may adversely affect their ability to make an informed choice.

Mackay (1995) says that participants may be naïve when it comes to video taping. The facilitator needs to ensure they understand the implications of giving permission to be video taped and how these recordings will be used. She points out that in some tests the video camera is left on throughout the session recording everything that happens, whether directly associated with the test or not. She suggests a sign be used that lets participants know when the camera is on and when it is not. This reminds them about the use of the camera and also gives them an opportunity to step out of the view of the camera, such as in breaks in the test session.

P4 Voluntariness

Professional demeanor influences participant involvement. This has implications in remote testing in particular, where people not trained in usability may be called upon to perform various functions during the test, such as assume the role of facilitator. Participants should not be rushed, nor should facilitators fidget while the participant reads the form. Coercion and undue influence should be absent when the person is asked to give their consent to participate in the test. Undue pressure might come in a number of subtle ways that one needs to be wary of. For instance, if you are in a position of authority over the participant such as employer to employee or teacher to student. Another subtle form of coercion is involved when participants receive payment for their participation. In the case of the latter it may be prudent to make the payment upfront, prior to the test. That way the participant will not feel pressured to have to stay to the end of the test (see P5 about the right to leave the test at any time).

A variation on this approach is that of Jarrett (2000). She says: “If the participant has been offered a financial incentive as part of the recruitment process, I hand it over immediately before explaining that

they can stop the test at any time without giving any reason. I felt that the knowledge that they hadn't received their incentive might inhibit them from leaving the test. If the participant is not aware of the incentive, then I leave it to the end."

P5 Participant's rights

Countries vary as to their recognition of human rights. Even where there is general agreement, definitions of those rights and interpretations of how they apply vary. Participants should have the right to be informed as to what their rights are. Karat and Karat (1997) reviewed the codes of ethics of 30 national computer societies and found that they shared 5 major topic areas. The first on their list "Respect" addressed the need to respect the rights of people involved with the technology, if for no other reason than for the prestige of the profession.

Dumas and Redish (1999), revealing a western bias, suggest rights most relevant to usability testing include the right to leave the test without penalty, the right to have a break at any time, the right to privacy (such as not having their names used in reporting the results of the test), the right to be informed as to the purpose of the test and the right to know before the test what they will be doing.

P6 Nondisclosure

When the product is under development or in any way confidential, participants need to be informed that they cannot talk about the product or their opinions of it. Dumas and Redish (1999) suggest giving participants appropriate wording that they can use to account for the time they spent in the usability test. Participants need to be informed about what they are permitted to divulge.

P7 Confidentiality

Confidentiality is different from the participant's right to privacy; it refers to how data about the participants will be stored. (Brankovic & Estivill-Castro (1999) define privacy as being to do with people and confidentiality being about data.) The ACS (2007) code stipulates that it is obligatory for members to preserve the confidentiality of others' information. The British Computer Society Code of Conduct does not specifically mention confidentiality or privacy, but states that members "shall have regard to ..." the legitimate rights of third parties, and have knowledge and understanding of relevant legislation, regulations and standards. Information in this case would be covered by the Data Protection Act (UK) and relevant regulations and standards, in the case of research, would be covered by the research funding councils in the UK. Amongst the principles for ethical research listed in the Economic and Social Research Council's research ethics framework (ESRC, 2007) (applicable in the UK) confidentiality applies to 'information supplied' and privacy is covered by the respect for anonymity of the participant. Mackay (1995) extends confidentiality also to who has access to video footage.

P8 Waivers

Permission needs to be obtained from participants to use materials such as questionnaires, audio and video recordings (and their transcripts). In many countries they have the right to refuse to give waivers. Participants should be given the option of having the data used for the purposes of the test, or of also having it used in a wider context. If the latter, then the consent form should state in what further ways the data will be used, so that an informed decision can be taken by the participant. At a minimum permission should be sought to use the materials for purposes relating to the evaluation of the product being tested. The actual wording will depend on numerous circumstances, such as local legal requirements and company policies.

P9 Legalese

Miller (1998) says that in software engineering informed consent documents should include measures of software quality. Measures that should be documented include margins for error, significant digits and rounding protocols, and these should be presented in unambiguous language. This should also become a principle for usability testing. It is too tempting to have legal departments draft the consent form. Just as software engineering terminology and legal jargon can hinder the signing of forms, so in usability testing such language does not make for rapport building prior the start of a usability test. Sensitive use on non-legal jargon should be made so that comprehension (P3) on the part of the participant is possible.

P10 Expectations

Globalization and related issues to do with international differences in culture and ethnicity lead to the notion of expectations. Each social grouping has its own means of resolving issues of power and hierarchy, turn taking, how interactions between people proceed, who can interrupt and contradict. There are accepted behaviors. Cultures interact through expectations. The level of familiarity with users that is acceptable in one culture for eliciting useful information may be deemed inappropriate in certain other cultures. For instance, privacy expectations vary, which has an impact on the use of recording media in a usability test.

Khaslavsky (1998) argues that misunderstanding in communication is common between people of the same culture (which is one reason for P9). She says such misunderstandings are magnified when dealing with people cross-culturally. Misunderstandings arise due to differences in work practices and social class systems. Yeo (1998) illustrates this with an example of a usability test conducted in Singapore, in which a participant broke down and cried. A post-test interview revealed that the participant's behaviour was attributable to the Eastern culture in which it is not acceptable to criticize the designer openly, because it may cause the designer to lose face. Yeo also cites examples of gender expectations that differ between cultures. In some cultures it is simply not appropriate to pair a man and a woman in a co-discovery design scenario. These are important considerations for product testing.

Conflict Resolution Among Principles

As is seen in the cases that follow, conflicts can arise between these principles. For example, case C2 shows conflict between the participant's rights to be informed about the purposes of the test and the company's rights concerning commercial in confidence matters.

The ACM/IEEE joint Code of Ethics (Gotterbarn, et al., 1999) states that in matters of ethical conflict 'public welfare' is the highest standard. A professional has a responsibility foremost to public welfare and professional judgment is needed to decide how this is best served in difficult moral decision making. The principle of minimal risk (P1) is the closest approximation of this for informed consent.

Given the heterogeneous nature of participants in usability testing, none of the other principles can be considered mandatory, they are instead discretionary, that is subject to contextual interpretation. Yet in most Western societies the first 4 principles fall into the "mandatory" category, because of legislative requirements and the codes of professional societies. However, even P1 has situation dependence. It is defined as minimal compared to 'normal' behaviour. But by this definition what is normal and hence of minimal risk to military personnel being tested on a new product may be considered very differently if one were testing primary school children of the same culture, even in the same city as the military personnel.

The Process Of Obtaining Informed Consent

Informed consent is both a process and a formal record of the process. That formal record is typically a form, but may also be another type of recording, such as video. Whatever the nature of the formal record entails, the consent given by the participant to proceed with the test must be recorded. Dumas and Redish (1999, p206) argue that: "If you are videotaping the test, have the camera(s) on while you are going over the form. The videotape shows that the participant was properly informed and voluntarily signed the form without pressure." However, whilst one sees the intent, this process is deficient. They are effectively recording the participant before the participant has given permission for this to happen. One imagines that if the participant chooses not to sign the form, that such a recording then becomes illegal in some countries; in such a situation the video footage of that participant should be destroyed.

The process of informed consent either begins on the arrival of the participant, by showing them the viewing room (if one exists) introducing observers, showing the equipment in the test room and generally building rapport. This also applies in remote testing situations that involve the use of distributed usability labs (Hammontree, et al., 1994). The process of informed consent can begin even earlier in the situation where participants are sent information (P2) about what will be expected of them ahead of their arrival. Neither the form nor the process ought to be vague about what the participant will experience (P2, P3). There should be a description given to the participant as to what the study is about, or if they are told then the facilitator should use a script so that each participant is

informed about the same things in the same way. This is needed to be sure that the participant can make a voluntary (P4) informed decision (P2) about whether or not to participate.

The consent form should state whether the data will be confidential (P7) or anonymous. However, the use of video often compromises principles of confidentiality (P7) and the rights of participants (P5) (Mackay, 1991; Mackay, 1995). Some participants will want to have a copy of the consent form, so provision for this eventuality should also be made. It might for instance be seen as one of the rights of a participant (P5). Finally as stated previously, the process of informed consent describes an attitude that begins when the facilitator greets the participant and continues until the participant leaves. This requires a professional, relaxed approach that is apparent to the participant right from the start.

Renegotiating informed consent

Miller (1998) does not encourage renegotiation of informed consent at a later date, though he says that allowance for this could be made. Case C2 below is an instance of where a company might deliberately pre-plan to renegotiate the agreement after the test. The morality of such a practice needs to be examined. One instance where renegotiation might ensue is presented by Mackay (1995) when video tapes are to be used for purposes other than were originally agreed to with the participant. Bentley (2000) has argued that the type of practice shown in case C2 is not deceptive but rather an example of deliberate misdirection. Bentley describes the need for a double consent procedure (discussed in more detail in the context of that case).

Cases

Though the following hypothetical cases could be used to address many issues in usability testing, the focus of the discussion after each case is on informed consent. The cases are adapted from Burmeister (2001).

Internet banking (C1)

An international bank, based in the United Kingdom, was testing a new internet banking product. They had a fully equipped usability lab in one of their Australian offices. Participants came to this lab to be tested and were introduced by the facilitator to the lab facilities and to a second person who along with the facilitator would be observing them. What participants were not told was that the product being tested had been developed by a Finnish team of software developers. Members of that team were remotely observing the tests being conducted using video conferencing facilities. When the developers in Finland had a question they would use the video-conferencing facility to ask one of the two people in the Australian observation room to ask the participant the question. This way the participant would not become aware that others were also observing the test. Bank management reasoned that this ensured the development team was properly informed concerning usability issues with their product, because the video conferencing facilities permitted them to observe the tests in near real-time, rather than viewing the video footage after the test. One of the things the site asked for was the participant's birth date. The purpose of this question was to verify that the user was at least 18, but the site didn't explain this. Users commented that the question was odd, though no one refused to answer it. [Note, participants were being paid to test the site.]

Because participants were not fully informed (P2, P5), they could not understand (P3) how the information being recorded about them would be used. Therefore principle P8 on waivers comes into this case in the sense that participants not being informed about the video link to Australia did not give permission to use the video recording for any purpose. If this were discovered by the participants (though that is unlikely), then the bank could face litigation. Perhaps the bank asked for permission to use video in the lab recording, but it is doubtful that such a (necessarily) vague permission relating to the use of video would save them from litigation. The video conference link that participants were not told about is also a violation of P7; there was no commitment to keeping participant data confidential.

P10 also comes into this case in the birth date situation. One should not assume that because certain age requirements exist in one country, that they also exist the same way in another. It may be that participants were confused because the age limit Finnish developers implemented did not apply in Australia.

Another principle that needs to be considered is P4. By paying for participation, are the results trustworthy? None of these participants refused to answer the birth date question, though they thought it 'odd'. Perhaps this is because they felt coerced through the payment. Had they not been paid, they may have refused to answer.

Double consent: Agents and Cookies (C2)

What are the policy implications when the test is specifically aimed at hiding information from the participant? For the following case assume that the financial institution concerned has approached your usability lab and asked you to organize the test. From an informed consent view point only, what are the policy implications?

Participants, who have previously shopped online and made purchases, are recruited for a usability test that they are told is to assess the look and feel of a number of online shopping sites controlled by a particular multinational company. The shopping experiences range from retail outlets, to entertainment and grocery shopping. Participants are given credit card details they are to use to make their purchases. However, the real purpose of the test is twofold. One is an initiative by a financial institution to test intelligent agents that are designed to identify and report fraudulent credit card transactions. That is, certain credit card numbers that were given to participants should have been identified by these agents. Also the shopping scenarios were scripted such that the agents should report on certain of the activities, but not on others. However, the financial institution does not want the public to become aware of their use of intelligent agents and therefore participants are not informed about this at all. Secondly, the sites that participants visit use a new form of cookies, that ought to quickly identify certain user behaviour, whether purchases are made or not, and target advertising to those users with increasing accuracy. For the purpose of this test it was deemed inadvisable to inform participants of the cookies ahead of their test. Then there are two alternatives. Under option A, a post test questionnaire asks participants about the advertising, informing them then or in a separate debriefing session about the use of the cookies. Under option B, participants are not informed at all about the use of the cookies.

At first one might object to this sort of testing as being dishonest or immoral. The participants are deceived from the beginning. Given the ethical codes of conduct in various countries this type of behaviour is unprofessional. However, there are many legitimate situations in which informing participants about the purpose of a test contaminates their behaviour. Usability specialists would argue that this process involves a degree of misdirection. That is, “how informed” does the participant need to be in order to observe P2 and P3? One study reported by Bentley (2000) used a double consent procedure that could be applied in circumstances such as in this case. That is (following option A) participants are informed at the end of the test about the use of cookies and asked to sign a second consent form. The risk here is that a participant may refuse to sign the second form, in which case Bentley says the data concerning that participant ought to be destroyed. Following this line of reasoning, deception is not involved, but rather some of the details are hidden (at least temporarily). This is deemed to be misdirection rather than deception or dishonesty.

As to the use of intelligent agents, one view could be that principle P6 on nondisclosure protects the company and therefore participants should be informed (P2) about the true nature of the test. In this case the informed consent form will need to be carefully written so that the company is indeed protected and procedures need to be put in place to ensure that participants understand (P3) the implications of this for them. This process should be done in a way that principle P9 concerning the use of non-legal jargon be observed.

Alternatively the bank could test their own employees, who as employees are bound by employment contracts to keep commercial in confidence material private. Mackay (1995) addressing the context of US video taping of employees in a usability test says that permissions to reuse the videos in any work related context is not required legally, given they were employees. Australian law likewise does not require the employer to obtain informed consent from the employee. However, Mackay makes the point that whilst this is not a legal requirement, it is not ethical (at least in her view).

CHALLENGES THAT THE HCI COMMUNITY FACES IN FUTURE DEVELOPMENTS

As computer technologies are introduced into what might be called ‘lifestyle’ settings. For instance, research on ambient technologies could be conducted in a number of different situations and locations to fully appreciate the impact of environmental influence – studies on location such as in the home or in medical institutions. It should be recognized that different settings could have an impact on the principles of informed consent – on the provision of information, on comprehension, voluntariness and expectations. It is important to consider whether participants are distracted by the setting they are in and whether they fully understand what is being asked of them. All the different locations mentioned above will have different characteristics in terms of distractions and power balances, and impacts

could vary according to the participant groups. Distractions may influence comprehension, and cultural behaviours may have an increased influence in settings that are 'familiar territory' for participants and where behavioural patterns are likely to be at their strongest.

More than the location changes, however, are the challenges posed by the technology itself, as different technologies converge, become seamless, invisible and 'intelligent'. We stated at the beginning of this paper that aspects of invisibility in programming and performance can raise ethical issues in respect of intended and unintended consequences such as in the case of invisible abuse and invisible complex calculations. In both of these instances the risk to the participants are greater as the visibility of the system itself (that is the artifact that presents the interface to the user) diminishes. In the case given above on Internet Banking (C1) the video conferencing situation was used by the development company who were not visible to the participants, and who did not announce themselves. The availability of invisible monitoring technologies (for example in Virtual Learning Environment applications), invisible observation (from remote systems, or in online chat rooms) allows access to data that users may be unaware of. Move these contexts to the home – where a strong case for monitoring elders in respect of their safety and health is actively promoted on the research agenda – and we have to be very careful how ethical research practices are managed. The temptation to utilize opportunities for data collection is strong – to many it represents efficient and best use of the situation presented and is not necessarily seen as unethical practice.

In the research context just given two issues relevant to ethical research are raised. The first is that our participants could now be classed as a vulnerable group, requiring special care and consideration. The second, not unrelated to the first, is how 'informed' will informed consent be? What of the level of comprehension? Is it necessary for the participant to understand the principles behind the technology (monitoring, transmission, storage) to be fully informed? An elderly user may easily comprehend the idea of, say, monitoring pill box use (to guard against overdose through forgetfulness for example) – but what of pressure sensors on a chairs, and radio tags embedded in household items and clothing that communicate with tag readers in floor mats, shelves, and walls? (Research proposed by Intel and described by Blanchard (2004).)

Consider the following vision of ambient technology applications:

"Humans are no longer the only intelligent decision makers on earth. Numerous decisions are being made by the visible and invisible microchips that are increasingly present everywhere in our working and living environment. Soon they will be hidden not only in our dishwasher and our mobile phone, but also in our furniture, clothing, shoes and walls. Ubiquitous computing is becoming a buzzword. All intelligent agents in our environment can make their own decisions. Continuously in communication with one another, they are guided by adaptive software to ensure that the result of their cooperation is a helpful, intelligent service to the user of the environment. These microchips are linked to a host of sensors, which minimizes the need for the users to interact with the computers. There is no need for keyboards or screens or menus. The intelligent environment has already heard what we said to the visitor, it has already noticed that we are leaving the building. The environment knows how it should behave, before we even think of giving an order. Such intervention greatly enhances our human comfort and our possibilities for managing the environment. Small tools can become active everywhere, even in our body. They can monitor, take over, correct or enhance our normal bodily functions. Numerous EU projects are developing the technology to realize this." (Van Steendam, et al., 2006)

So how will informed consent and usability testing look in this context of invisible computing? At one level probably not so different – informing the participant involves a description of the task to be accomplished in a given setting. The extent to which technical detail is conveyed may simply depend on its relevance to the task in hand, and to grounding user expectations. However, the detail of user interaction will undoubtedly change removing the user from the monitor/keyboard or mobile phone/PDA type of device. What is usability testing where there are no "keyboards or screens or menus"? How do we manage testing biometric interfaces? If our home, car, medical technologies rely on biometric input, for example to establish the personal profile of the user, will the user understand the implications? (In terms of security of data, or national data collection schemes).

The case of double consent given in the previous section discussed the use of agents and cookies (C2). In the ambient context agents are envisaged as playing a significant role, and in many cases the context relies on a personal profile (as collected currently by cookies). A similar situation as C2 could arise where intelligent agents operate in the background collecting information concerning behaviour

and/or attitudes, but the researchers would not want to disclose this at the outset (to avoid influencing the research). A positive attitude may seem important to the researchers in gaining the co-operation of the participants, and encouraging an acceptance of the technology (which could have a positive impact on perceived usability). In many instances these home technologies are being designed for assisting the older population to maintain independence. They may wish to test participants' ability to cope with increased complexity, and only reveal the requirements of the task at a superficial level to begin with, increasing complexity as the study progresses. At what point is renewed consent required or desirable? And what is the 'required' or 'desirable' benchmark?

In many instances these home technologies are being designed for assisting the older population to maintain independence. The participants may have been informed of the beneficial effects of such a technology in their homes and be encouraged to test it with this in mind. These are not necessarily misdirected instructions, but without an understanding of the ways in which the technology is working, or any idea of what may be going on behind the scenes, informed consent in the test situation is based on a purely functional view of the technology rather than placing it in a wider context. When processes are out of sight we are likely to either ignore them, or be unaware of them. In both cases these are usually classed as the benefits, if not the purpose, of computers – that is, to take the cognitive load off the user. Designers can choose to enhance or reveal “invisibility” – dialogue boxes for example reveal occurrences in programs often warning that something is wrong. Dialogue boxes characteristically offer the user choices, but users often (a) do not understand the terminology or the context given and (b) are unaware of their choices (for instance, in rejecting “cookies”). Will researchers want to re-instate some cognitive burden in order to fully inform their users?

Providing the wider context would not only enhance the experience for the participant, but also educate them in the technologies that may be underpinning their lives. In other words, there is an opportunity to extend the test situation to 'value added' research.

CONCLUSION

Informed consent procedures raise the level of public trust in the process of the whole usability test. It is part of a quality process that is required to successfully bring a product to market. For HCI researchers to get honest and reliable feedback from participants, those participants need to be able to trust the company or research organisation, and the people administering the test. Informed consent procedures go a significant way towards ensuring that trust is established and maintained.

We have noted some of the challenges for the HCI community in the future, both in terms of their practice with regard to meeting their obligations to the research participants and the changing context and interface presentations and modalities. As the technology becomes less obvious, so the temptation to provide only the necessary information increases. Indeed, a purely innocent lack of awareness regarding the implications of the data collected can have consequences for the participant and decisions may need to be made post test whether to revisit the participant for further consent or elaboration. The professional engaged in this type of research has responsibilities that extend beyond simply meeting requirements, either of ethics committees or the law. Introducing new technologies into a population who are ill-informed will not only have an adverse effect on feedback, but is opening the door to a level of distrust of new technology and of the professions behind the technology. Informed consent seeks to 'fully inform' and interpretations can vary as to whether participants should simply be informed of the task at hand, or given more detail. It has been argued in the previous section that especially with disappearing technologies users should be briefed on the technology, its capabilities, the behind the scenes operations (in non-technical terms) in order for them to be able to engage with the technology at the proper level – and with the knowledge they need to be a real 'participant' in a study, rather than someone who fits the description of user and is a number for the research statistics.

In concluding it is worth repeating that informed consent is more than policies, process and principles, it is an attitude that begins when the facilitator greets the participant and continues until the participant leaves.

Developing technologies and new contexts raise research issues that can take us by surprise – social studies into Internet Chat rooms are a classic example that have raised issues of covert observation and misrepresentation. In light of previous experience we should be giving some thought now to the issues that we are likely to face with the next level of ubiquitous, pervasive and invisible technologies.

REFERENCES

- ACS (2007) Code of Ethics, <http://acs.org.au/index.cfm?action=show&conID=coe>, accessed 22/3/07.
- APA (1997) APA Statement on Services by Telephone, Teleconferencing, and Internet, <http://www.apa.org/ethics/stmnt01.html>, accessed 22/3/07.
- BCS (2007) Code of Conduct, available from: <http://www.bcs.org/server.php?show=nav.5651>, accessed 31/3/07.
- Bentley, T. (2000) Biasing Web Site User Evaluations: A Study, Proceedings of the Annual Conference of the Computer-Human Interaction Special Interest Group (CHISIG) of the Ergonomics Society of Australia, Sydney, Dec.
- Blanchard, J. (2004) Ethical Considerations of Home Monitoring Technology, reprinted from the Home Health Care Technology Report, v1(4):53,63-64, 2004. Civic Research Institute.
- Brankovic, L. & Estivill-Castro, V. (1999) Privacy Issues in Knowledge Discovery and Data Mining, Australian Institute for Computer Ethics Conference, Lilydale: Swinburne University of Technology, July, 89-99.
- Burmeister, O. K. (2001) Usability Testing: Revisiting Informed Consent procedures for testing internet sites, Conferences in Research and Practice in Information Technology, Vol 1, 3-10.
- Commonwealth of Australia (1999) National Statement on Ethical Conduct in Research Involving Humans, Canberra: AusInfo Publishing.
- Dumas, J. S. and Redish, J. C. (1999) A practical guide to usability testing, Exeter, England: intellect.
- Economic and Social Research Council (ESRC) Research Ethics Framework (2007) available at: www.esrcsocietytoday.ac.uk/ESRCInfoCentre/
- Gotterbarn, D., Miller, K. and Rogerson, S. (1999) Software engineering code of ethics is approved, Communications of the ACM, 42(10), Oct., 102-107.
- Hammontree, M., Weiler, P. and Nayak, N. (1994) Remote usability testing, ACM Interactions, 1(3), 21-25.
- Jarrett, C. (2000) personal communication, Thursday, September 7th.
- Karat, J. and Karat, C. (1997) World-Wide CHI: Future Ethics, SIGCHI Bulletin, 29(1), January.
- Khaslavsky, J. (1998) Integrating Culture into Interface Design, Proceedings of the conference on CHI 98 summary: human factors in computing systems, April, 365-366.
- Mackay, W. E. (1991) Ethical issues in the use of video: Is it time to establish guidelines? CHI '91 Conference Proceedings, Louisiana: ACM Press, April, 403-405.
- Mackay, W. E. (1995) Ethics, Lies and Videotape..., CHI '95 Conference Proceedings, ACM, <http://sigchi.org/chi95/Electronic/documnts/papers/wem1bdy.htm>, accessed 31/3/07.
- Miller, K. (1998) Software informed consent: docete emptorem, not caveat emptor, Science and Engineering Ethics, 4(3), July, 357-362.
- Moor, James H., (1985) "What is Computer Ethics?" in Metaphilosophy, 16(4).
- Sanderson, P. (2000) Human-Computer Interaction lecture series, Hawthorn: Swinburne University Of Technology, April 18th.
- Van Steendam, Guido., Andras Dinnyes, Jacques mallet, Rolando Meloni, Carlos Romeo Casabona, Jorge Guerra Gonzalez, Josef Kure, Edors Szathmary, Jan Vorstenbosch, Pter Molar, David Edbrooke, Judit Sandor, Ferenc Oberfrank, Ron Cole-turner, Istvan hargittai, Beate Littig, Miltos Ladikas, emilio Mordini, Hans E. Roosendaal, Maurizio Salvi, Balazs Gulyas, Diana Malpede (2006) Report: The Budapest meeting 2005, Intensified networking on Ethics of Science, The Case of Reproductive Cloning, Germline Gene Therapy and Human Dignity. Science and Engineering Ethics, Vol. 12, No. 4, 2006. Excerpt: 731-793.
- Yeo, A. (1998) Cultural Effects in Usability Assessment, Doctoral Consortium, Proceedings of the conference on CHI 98 summary: human factors in computing systems, April, 71-75.

COPYRIGHT

Duquenoy and Burmeister ©2008 The authors assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

Encouraging Ethical Decision Making in Security Policies

A.B. Ruighaver

School of Information Systems
Deakin University
Melbourne, Australia
Email: ruighaver@optushome.com.au

Extended Abstract

While there is extensive literature on the positive effects of institutionalising ethics in organisational culture, our extensive research in information security culture has found no evidence of organisations encouraging ethical decision making in situations where information security might be at risk. Security policies, in particular acceptable use policies, have traditionally been written with a strategy of deterrence in mind, but in practice they rely mostly on deontological ethics, i.e. employees doing the right thing, to work. Actively enforcing deterrence by increased monitoring of behaviour and severe punishment of unacceptable behaviour would, in most cases, be detrimental to the general organisational culture, and should therefore only be used to control the most critical of risks. As far back as 1990, evidence has been reported of a widening socio-technical gap, where employees no longer always act according to expected social norms in an organisation. Together with a widening technical control gap in information systems, largely due to the growing complexity of IT infrastructure, this change in moral behaviour is reducing the effectiveness of security policies in an organisation and driving the need to support decision making based on consequential ethics. In consequential ethics the ethical value of an action is determined by the outcome, even though the action itself may not be ethical. In this paper, an alternative approach to the development of security policies is proposed to encourage ethical decision making based on consequential ethics. Obviously, the need to ensure that employees understand how to deal with ethical issues will, in general, have to be addressed by other means. But, we believe that it is important that security policies emphasise the risks that they try to control as well as the unintended negative consequences of an employees actions when that employee decides to ignore any guidelines in the security policy. While one cannot solely rely on the security policy itself to increase the employees awareness of security objectives and possible risks, it is important that the policy is written so that ethical decision making in information security is consistently supported. It is no longer sufficient to just emphasise deterrence by listing the punishments the organisation can apply when its guidelines are not adhered to. To encourage ethical decision making, guidelines will need to be written in such a way that the policy continuously acknowledges that employees are no longer expected to blindly follow these guidelines, and that these guidelines will not cover all the possible risks related to an employees behaviour. Both explicitly and implicitly the policy will need to emphasise that employees are expected to make an ethical judgement of all actions that may possibly endanger the organisation's security.

COPYRIGHT

A.B. Ruighaver©2008 The author(s) assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

Developing professional ethics through game design and role-play with the Pirate's code of conduct

Ken Eustace

School of Computing & Mathematics

Charles Sturt University

Wagga Wagga, Australia

Email: keustace@csu.edu.au

Abstract

Scuppers Island is a role playing game (RPG) project based on a pirate code of conduct as the major part of the game play. In an educational context, game-based learning is used to teach computer ethics which can be extended to professional ethics. The purpose of the game is to let the players interact as pirates and learn about values, ethics and differences in each other's ethical beliefs. To design the game, games design theory was researched and implemented using a set of basic rules. A game must have a hero, and must involve a quest or challenge, for it to be an effective learning tool. The project team members propose that use of an online environment in teaching professional ICT ethics can be very effective if used in conjunction with traditional learning techniques.

Keywords

Artificial Intelligence, Autonomous Agents, Computer ethics, Eliza Bot, Pirate code of conduct, Role Play, Role Playing Game, Virtual Worlds.

INTRODUCTION

Scuppers Island is a role playing game (RPG) at <http://ispg.csu.edu.au:7688/> (Figure 1). Role play as a student centred experiential learning activity has been a characteristic of teaching and learning environments for many years (Jones 2007, Loui 2006, Brown, 1994). Developments in Web programming have also enabled the design of media-rich role play environments in which learners deal with the complexity and ambiguity of real life ethical issues and the same time develop their knowledge and self-efficacy with online communication.

enCore Xpress 4.0.1


Copyright (C) 1997-2004
enCore Open Source Project,
All Rights Reserved

This program is Free
Software and comes
WITHOUT ANY WARRANTY!

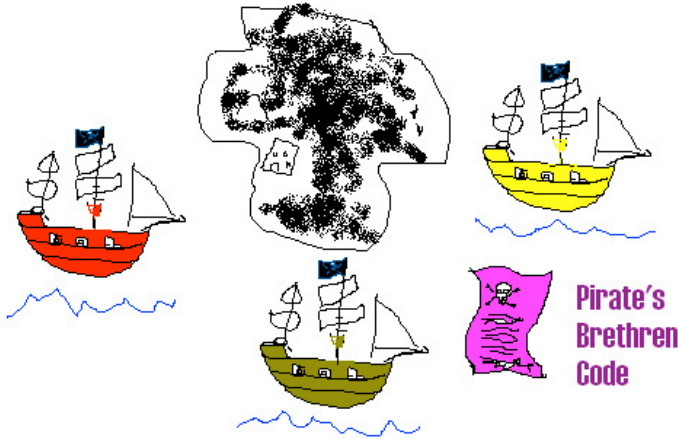
User ID

Password

[System Requirements](#)



Scupper's Island



Pirate's Brethren Code

A role playing game (RPG) using the pirate code of conduct.

It is the year 1642, me hardies, to our little spot in the Carribean. The outer shoreline of Scuppers Island, there be Galleon Reef; Cutlass Bay; Ransom Cove; Point Bowsprit and Buccaneer Lagoon. The sea shanty village of Port Brigantine (on Cutlass Bay) and the restful Hogshead Tavern is where the Pirate ship crews meet. The island is mostly bare 'cept for Spyglass knoll a mountain with caves that overlooks Galleon reef and if ye wander far off to the other side, ye be careful going near Mad Ben Tankards treehouse on Buccaneer lagoon!

Best of luck to ye and hope you keep clear of Davy Jones or the curse of the black spot!

19 September each year is 'International Talk like a Pirate Day'...arrgghh so talk it up me hardies!

Figure 1: The Scupper's Island Login Screen- ispg.csu.edu.au:7688

Ethics, software development, game design and play

Eustace, Mason & Swan (2007) devised the learning experiences at Scupper's Island to occur on many layers, Students work at one or more tasks in software development, game design and as players who interact with each other and objects in an EnCore learning environment (Holmevik & Haynes, 2000). EnCore was selected due to the ability to facilitate user-centred virtual reality and play through its object oriented programming tools and can be downloaded from <http://encore-consortium.org/>.

The pirate code of conduct and research into games design theory are used in order to design, build and play the game by students and the teacher-researcher using bot programming. Bots are robot programmes that respond to messages and bring back answers or do data mining. They have been used as agent software in artificial intelligence (AI) and as chatter bots to mediate chat services.

In every online community, there is a code of conduct. From discussion boards, to virtual worlds, there is nearly always a mediator who over-looks all discussion. If a code has been broken, then it is up to this mediator to deal with the offender. As role-play gamers, students will increase awareness and understanding via bot programmes of their own personal ethics and professional ethics as well as the ethical nature of online learning with an RPG as a common context for all modes of learning.



Additionally as software developers of parrot bots, acting as ethical agents, participants examine the issues and ethics concerning artificial intelligence and software agents. This form of active learning complements the more theoretical approach in learning about professional ethics in the ICT industry and elsewhere.

THE GAME SCENARIO

Scuppers Island is set in the year 1642, about the same period when the brethren of the coast formed a democratic community. They held a code based upon the Pirate code of conduct, which was the social contract or code of conduct for each voyage. The captain and officers were elected and every decision of importance was discussed, followed by a vote. The game can use up to three different pirate ships, each with different codes of conduct, in order to pose a dilemma situation to the player as well as conflicts between the ship members due to the differences in their codes.

Scuppers Island is the home for three pirate ships somewhere in the Caribbean Sea. Each ship is run under similar but different variations of the Pirate code of conduct. Players are divided into members of three ships called the Sea Dragon, Golden Tiger and Storm Queen – each with a separate governance style (dictatorship, democracy or anarchy) and version of the pirate code, as shown in Figure 3. The codes avoid rules against women that the 1642 pirates had, so that any gender bias for players is removed.

Sea Dragon Code



Sea Dragon (Dictatorship): has the most rules and is a very strict code where all orders are given by the captain and the crew have no right to vote against him.

- 1: Ye Captain shall have full command at all times. He who disobeys will be punished.
- 2: Ye Captain shall receive one share and a half of spoils. Officers shall receive one share unless ye distinguish yourself in which spoils will be decided by ye crew
- 3: Spoils taken from a captured ship shall be distributed equally
- 4: If ye lose an eye, hand or leg, ye shall receive up to six slaves or six hundred crowns
- 5: Ye supplies and rations shall be distributed equally
- 6: If one brother steals from another, his nose or ears are to be cut off. If he sins again, he is to be given a musket, bullets, lead and a bottle of water and marooned on an island.
- 7: Quarrels between several brothers whilst aboard ye ship shall be settled ashore with pistol and sword. He that draws first blood shall be the victor
- 8: All ye who shall plot to desert, or having deserted shall be captured, and be given a musket, bullets, lead and a bottle of water and marooned on an island.
- 9: Any brother who is being lazy or fail to clean his weapons shall suffer 40 lashes
- 10: Gambling is strictly forbidden, and is punishable by 40 lashes
- 11: Ye who carry a bare flame on board the ship shall suffer 40 lashes.

Figure 2: The Sea Dragon's strict code

The ships come together often between voyages to celebrate their recent ventures at the Hogshead Tavern, owned by former pirate, Tom Flint (Figure 3). Tom is the author's own character and the administrator of Scupper's Island. Each ship has its own Macaw parrot (bot), which recounts the code of conduct signed by each of the ships company. The parrot bot is an implementation of an Eliza-like Turing bot (Turing 1950, Weizenbaum, 1966) that is designed to pick up keywords that may represent a violation of the pirate code.

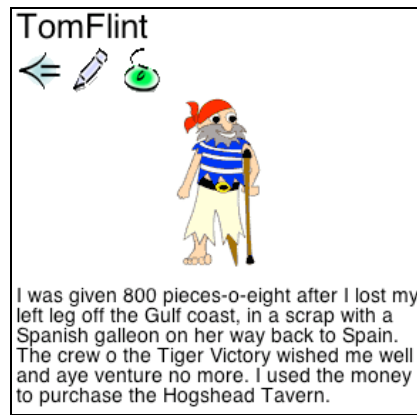


Figure 3: Player profile of Hogshead tavern owner, Tom Flint.

There is a dark corner in the tavern, where people signed up to ships for the next voyage.

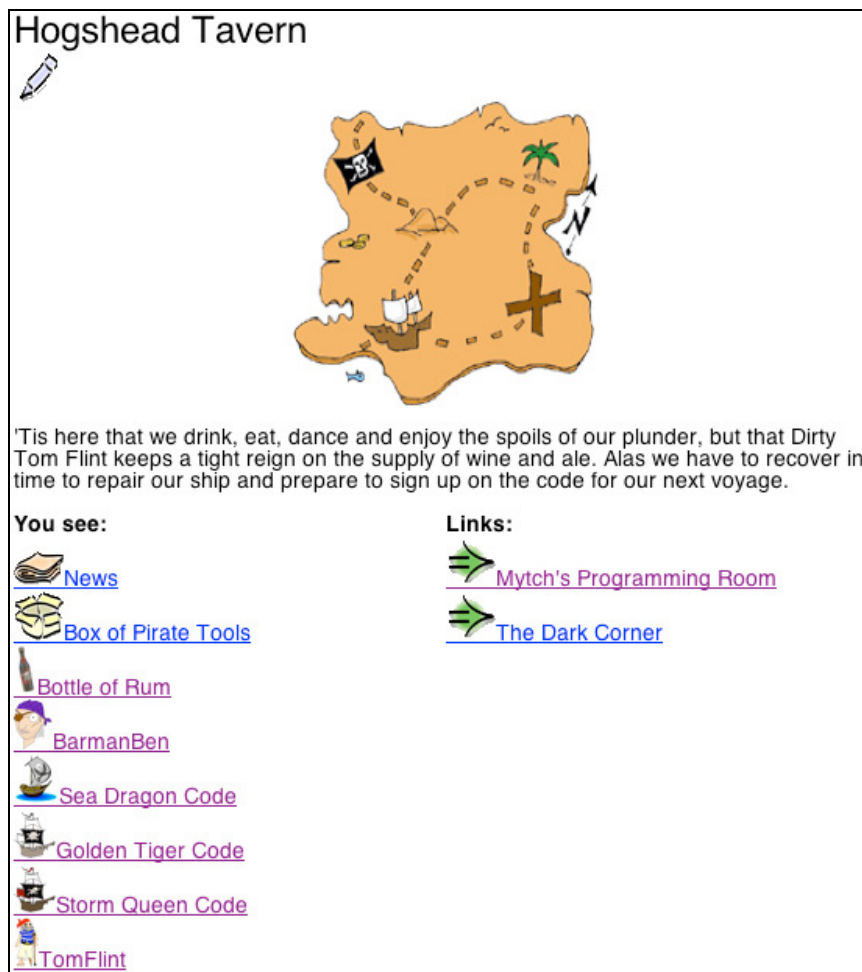


Figure 4: Hogshead Tavern Welcome Screen- ispg.csu.edu.au:7688/62/

A tavern bot called BarmanBen (Figure 5) will serve drinks to the thirsty pirates, and a wise sage bot will tell the players why they should accept the mission of signing onto a ship, using deontic logic where possible during interaction with the players. Mally's Deontic Logic (Goble, 2005) was proposed as a form of logic using modal operators to describe obligation and permission as a type of pure ethics. This will be a challenging ethical framework to develop as it requires input from experienced ethicists and programmers. The two bots in the Hogshead Tavern will need to be able to communicate

with the players effectively, and keep them interested, while the three parrot bots re-enforce the code of conduct of each ship.

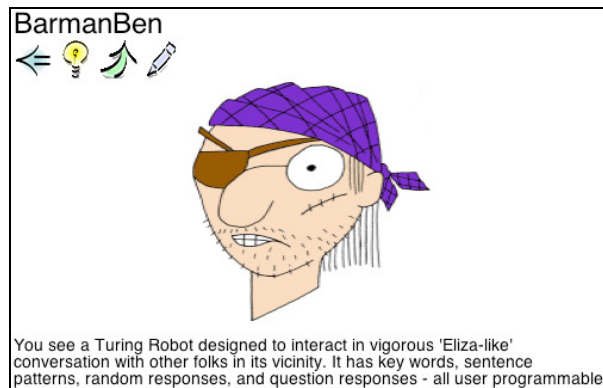


Figure 5: BarmanBen – the tavern bot

THEORETICAL FRAMEWORK

The role play game evolves each time it is played. Games-based learning using role play design shares the same theoretical background as suggested by previous research: Gee (2004); Papert (1998) and Reiber (1996). Lee et al ((2005) applied the work of Gikas & Van Eck (2004) to show that an RPG active learning experience develops the learner within the five intellectual skills of Gagné as well as all six levels of Bloom's taxonomy of the cognitive domain. By its nature, brainstorming an ethical dilemma is player-centred and requires high order problem solving and critical thinking skills to resolve. In teaching professional ethics, other uses of role play exist in teaching business and engineering ethics but not using an online RPG (Brown 1994 Loui 2006). The special case with the Scupper's Island RPG website is that players learn by both design and play.

The role play design begins with description of the stakeholder pirate ships, as suggested by van Ments, (1999). Coupled to game-based learning theories is game design theory. The Jungian model of storytelling using the 'hero' approach was selected (Campbell, 2001) as it revealed the number of steps that a game must have if it is to have a positive impact on the player. Cooper (1996) described four ethical layers of respect, responsiveness, caring and moral goodness that apply to online gamers and suggests the each member should be mindful of these ethical layers during game play.

PROCEDURES USED TO TEST HYPOTHESES

From the literature search and the theoretical framework emerged the hypothetical ideas behind this games-based learning study by focusing on testing the educational value of the RPG:

1. *Does game design and play offer an effective deep learning experience in professional ethics?*
2. *Does the RPG improve the learning outcomes of professional ethics when used in conjunction with face-to-face or traditional teaching practices?*

To test these hypotheses, several procedures will be performed over several teaching sessions from August 2008 to 2010. An overview of the data collection methods from a review of the literature and analysis of the game dialogue and server logs is determined. Participant surveys will gain some statistical data to back up the results. This study so far found no quantitative data from previous studies by Foner (1993) or Mowbray (2002) to show how effective online or games-based learning is opposed to traditional learning in professional ethics.

PEDAGOGICAL BASIS OF BOT PROGRAMMING

Bjork (2004) described how Bot programming has several contexts for educational use through moderation of group discussion, simulation, mentoring and guiding which help to set ideas in an individual context for the learner. The project began with research into games design, codes of conduct, deontic logic and Eliza-like bots, based on the early works in artificial intelligence like Allan Turing's Turing Test (Turing, 1950) and Weizenbaum's Eliza programme (Weizenbaum, 1966).

Conversational bots are designed to convince the player that they are human by picking up patterns in their speech and rearranging them to make it seem like it is forming a conversation.

Parrot Bots: Enforcing the Rules of Engagement

A functional bot is used to enforce a code of conduct in the game environment. In online communities rules are often hard to enforce as the participants often reject these forms of online government. So by implementing a bot to detect possible violations of the code the players can be constantly reminded of the rules that are involved to belonging to that online community. In this way, the players not only learn about ethics but also differences in each other's ethical beliefs.

Each ship has a parrot bot that will act as a reminder of that player's code of conduct. The game centers around 3 different pirate ships with 3 different codes of conduct, each of which is designed to pose ethical dilemmas to the player as well as conflicts between the ships due to the differences in their code. A master set of rules for each ship's pirate codes was established and then certain rules are taken out for each of the pirate ships and are available as a note objects 198-200 inside the Hogshead Tavern at <http://ispg.csu.edu.au:7688/62/>.

BluePrint: Parrot Bot Prototype class

To program each bot to recite the code, two aspects had to be addressed: reading what the player has said and detecting whether it relates to one of their rules as a pirate and making the parrot bot appear parrot-like and realistic inside the game's environment. To do this a parent parrot class was made called BluePrint which was programmed to respond to all of the rules regardless of which code they belong to as well as appear to be parrot-like. BluePrint is not designed to be used inside the game, instead the purpose is to provide a class on which the game parrots are made. BluePrint can be tested inside "Mytch's Programming Room" (<http://ispg.csu.edu.au:7688/175>) in Scupper's Island.

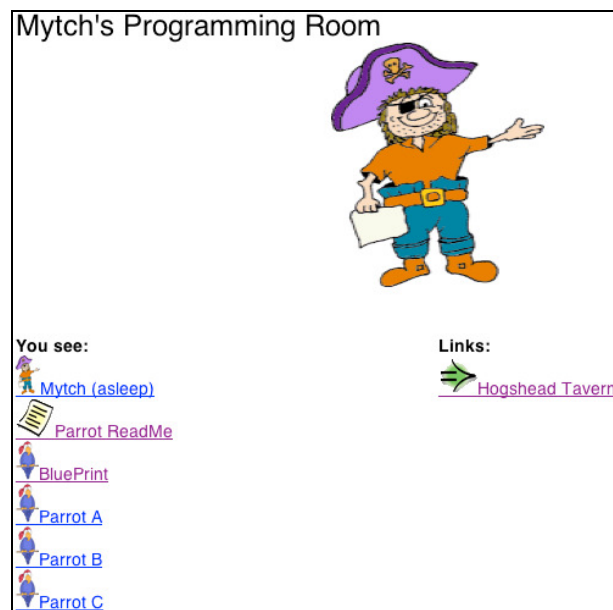


Figure 6: Mytch's programming room test each bot prototype.

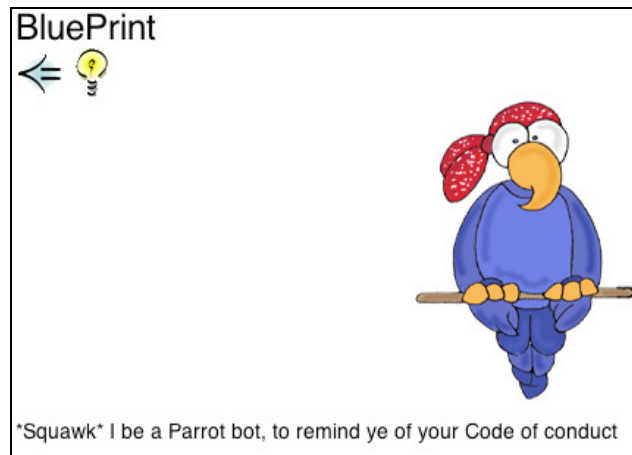


Figure 7: The parrot bot called Blueprint

Programming Code

To program the parrots to respond to breaches in the code of conduct keywords were used to detect when the player is talking about something relevant to their code. These keywords in Figure 8 only reflect rule 1, where if the player was to mention either disobey, order or captain inside the game the parrot would then interrupt and remind the player that “ye captain shall have full command at all times” which helps to ensure that the players remember and obey their code of conduct. For a comprehensive list of all the keywords used please have a look a note objects 198-200 inside the Hogshead Tavern.

KEYWORDS:

1 disobey

Squawk Ye Captain shall have full command at all times. He who disobeys will be punished.
Punishments may be overturned by a majority vote

Figure 8: The parrot bot called Blueprint

Realism

Another key issue when programming a bot is concerned with making sure that it has its own identity inside the game. The parrot had to be made to sound authentic to the player so two techniques were used:

- Placing the word *Squawk* in every sentence from the bot reminds the player that it is a parrot talking. Parrots in real life often mimic what is said to them.
- Each bot uses several lists to create an authentic conversation: a list of pattern rules used to help create authenticity; a list of keywords that evoke use of a pre-stored response and a list of random responses to stimulate discussion.

Each bot used is designed to respond to all messages that are said in the room, but one problem to fix is when to make the parrot not say something, as a noisy parrot may become quite annoying during the game play.

CONCLUSION

The six unique features of Scupper's Island RPG as devised by the project team is described in Table 1.

1	Players learn by design and play and the RPG is extended each time it is played.
2	Game design theory and the Jungian 'hero' approach as the core design (Campbell 2001)
3	Independent, collaborative and experiential learning opportunities exist in ethics, software development, game design and online role play.
4	Mally's Deontic Logic (Goble, 2005) extends the ethical framework inside the RPG
5	Conversational Eliza/Turing bots (Turing 1950, Weizenbaum, 1966) includes computer science and programming skills and RPG mentoring and guidance (Bjork, 2004).
6	Awareness of the four ethical layers during online game play as respect, responsiveness, caring and moral goodness . (Cooper ,1996)

Table1: Unique features in the design of Scupper's Island RPG

Role play cannot be done by educators in isolation, according to Project EnRole – a Carrick Institute funded two-year project (<http://cedir.uow.edu.au/enrole/>). Wills et al (2007) described project EnRole as a vehicle that will assist those teachers using role play in Australian universities. Apart from providing support on workload and recognition, the major resource being developed is a repository of sharable/reusable role play learning designs with an associated peer review process. Scupper's Island will be part of that repository and seek further support from both project EnRole and any interested colleagues interested in using online role play in university teaching.

Any game, or virtual world used in an education context, is effective if used in conjunction within a sound learning context. The popularity of social networking sites like SecondLife, MySpace and Facebook, demonstrate a student willingness to participate with others and could be argued that they exist as a type of social role play/business model, with its own ethical issues to deal with on a massive scale, as well as building role play skills in the membership that assist in learning.

The Scupper's Island RPG will continue to evolve and can be used in conjunction with learning in a theme, topic or subject on professional ethics. The game is complementary to other experiences, not a replacement to them. Together, most students will get a chance to have a say, and be comfortable in putting forward their views in response. The reader can use a guest login to Scupper's Island to visit the working prototype at <http://isp.g.csu.edu.au:7688/>.

Effective use of games-based learning in the traditional, online or blended learning situation is the aim of Scupper's Island RPG. While teaching ethics in a traditional classroom, the quality of participation from students may be higher than online as it is easier to engage in a debate; encourage valuable quick-thinking skills and is easier to perform and absorb do presentations. However there are some positives for teaching in an online classroom using online games as students with obligations enjoy the flexibility of online classes, particularly as the majority of students in distance classes are working toward a higher degree. Students learn more about their fellow students and participation increases in online classes. In addition the RPG can arouse interest, motivate students, be re-played and the design extended at a later date.

REFERENCES

- Bjork, O. 2004, *MOO bots*, [Online. internet], Available: , <http://www.encore-consortium.org/Barn/files/docs/moo-bots-040505-4.pdf>, Accessed 01 Nov. 2007.
- Brown, K.M. 1994, Using role play to integrate ethics into the business curriculum: a financial management example, *Journal of Business Ethics*, Vol .13, No. 4, pp.105 – 110.
- Dunnigan, J F. 1997, *10 Steps to Designing*, [Online. internet], Available: , http://www.alanemrich.com/PGD/Week_02/PGD_Ten_Steps.htm, Accessed 27 Oct. 2007.
- Campbell, J. 2001, *A Practical Guide to THE HERO WITH A THOUSAND FACES*, [Online. internet], Available: <http://www.skepticfiles.org/atheist2/hero.htm>, Accessed 27 Oct. 2005.

- Cooper, E. W. 1996, *Wizards, Toads and Ethics: Reflections of a MOO Administrator*, [Online. internet], Available: , <http://www.december.com/cmc/mag/1996/jan/cooper.html>, Accessed 01 Sep. 2007.
- Eustace, K, Mason, C. & Swan, M. 2007, Scupper's Island: Using game design and role play to learn about professional ethics. In *ICT: Providing choices for learners and learning. Proceedings ascilite Singapore 2007*.
- Foner, L, 1993, *What's an Agent, Anyway?: A Sociological Case Study*, [Online. internet], Available: <http://foner.www.media.mit.edu/people/foner/Reports/Julia/Agents--Julia.pdf>, Accessed 11 Oct. 2007.
- Gee, J. P. 2004, Learning by design: Games as learning machines. Paper presented at the *Game Developers Conference*, San Jose, CA, March 22-26. [Online. internet], Available: http://www.gamasutra.com/gdc2004/features/20040324/gee_01.shtml, Accessed 29 Apr. 2005.
- Goble, L. 2005, A logic for deontic dilemmas, *Journal of Applied Logic*, 3, 3-4, pp 461-483
- Gikas, J. & Van Eck, R. 2004, *Integrating video games in the classroom: Where to begin?* Paper presented at the National Learning Infrastructure Initiative 2004 Annual Meeting, San Diego, CA, January 25-27. [Online. internet], Available: <http://www.educause.edu/ir/library/pdf/NLI0431a.pdf>, Accessed 29 Apr. 2005.
- Holmervik, J R & Haynes, C. 2000, *MOOniversity: A Student's Guide to Online Learning Environments*. Boston: Allyn and Bacon.
- Jones, S. 2007, Adding value to online role-plays: Virtual situated learning environments. In *ICT: Providing choices for learners and learning. Proceedings ascilite Singapore 2007*. [Online.internet], Available: <http://www.ascilite.org.au/conferences/singapore07/procs/jones-s.pdf>, Accessed 19 Dec. 2007.
- Laramée, F D. 1999, *GameDev.net - The Game Design Process*, [Online. internet], Available: <http://www.gamedev.net/reference/articles/article273.asp>, Accessed 27 Oct. 2007.
- Lee, M. J. W., Eustace, K., Fellows, G., Bytheway, A. and Irving, L. 2005, Rochester Castle MMORPG: Instructional gaming and collaborative learning at a Western Australian school. *Australasian Journal of Educational Technology*, 21(4), 446-469. [Online. internet], Available: <http://www.ascilite.org.au/ajet/ajet21/lee.htm>, Accessed 27 Oct. 2007.
- Leonard, A, 1997, *Bots: The Origin of New Species*. San Francisco: Hard Wired, 1997.
- Loui, M. C. 2006, *Role Playing in an Engineering Ethics Class*, Online Ethics Center for Engineering, National Academy of Engineering, [Online. internet], Available: <http://www.onlineethics.org/CMS/edu/instructguides/loui2.aspx>, Accessed 01 Nov. 2007.
- Mathis, D J. 2005, *Learning Online: A Resource for Students on the Virtual Classroom*, University of Wisconsin-Milwaukee, [Online. internet], Available: <http://www.uwm.edu/People/djmathis/traditionalvsonline.html>, Accessed 25 Oct. 2005.
- Mowbray, M. 2002, Ethics for Bots. Paper presented at *14th International Conference on Systems Research, Informatics and Cybernetics*, Baden-Baden, July29-Aug3, [Online. internet], Available: <http://www.hpl.hp.com/techreports/2002/HPL-2002-48R1.pdf>, Accessed 12 Oct. 2007.
- Papert, S. 1998, Does easy do it? Children, games, and learning. *Game Developer*, 5(6), 88.
- Peabody, S. 1997, *The Art of Computer Game Design- Chapter 5*, Washington State University, [Online. internet], Available: <http://www.vancouver.wsu.edu/fac/peabody/game-book/Chapter5.html>, Accessed 27 Oct. 2005.

- Richard Rouse III and Wordware Publishing 2004, *Game Design: Theory & Practice*, Wordware Publishing, [Online. internet], Available: <http://www.paranoidproductions.com/gamedesign/about.html>, Accessed 26 Oct. 2005.
- The Depot and News & Record Online 1997, *BlackBeard Lives*, [Online. internet], Available: <http://www.blackbeardlives.com/day3/code.shtml>, Accessed 26 Oct. 2005.
- Turing, A, 1950, Computing Machinery and Intelligence. *Mind*, 59.
- van Ments, M. 1999, *The Effective Use of Role-Play: practical techniques for improving learning*, London, Kogan Page.
- Weizenbaum, J. 1966, ELIZA—A Computer Program For the Study of Natural Language Communication Between Man and Machine." *Communications of the ACM* , Vol. 9, No. 1. pp. 36-45.
- Wills, S., Devonshire, E., Leigh, E., Rosser, E., Shepherd, J. & Vincent, A. 2007, Encouraging role based online learning environments. In *ICT: Providing choices for learners and learning. Proceedings ascilite Singapore 2007*. [Online. internet], Available: <http://www.ascilite.org.au/conferences/perth07/procs/wills-roleplay-symposium.pdf>, Accessed 27 Dec. 2007.

ACKNOWLEDGEMENTS

Prof. John Weckert, Oliver Burmeister, Geoff Fellows, Clinton Mason and Mitchell Swan from Charles Sturt University.

COPYRIGHT

Ken Eustace ©2008. The author assigns the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

A Theoretical Framework for Academic Integrity

Kay Fielden

School of Computing and Information Technology

Unitec New Zealand

Auckland, New Zealand

Email: kfielden@unitec.ac.nz

Abstract

In a global academic culture operating within a managed higher education climate in which institutional funding is implicated by research represented by final outputs (usually written documents), maintaining academic integrity in computing for all stakeholders has become an issue. In this paper a multi-stakeholder, multi-level theoretical framework is proposed in which the current literature on academic integrity in computing can be situated.

Keywords

Academic integrity, Plagiarism, Managed higher education, Professional standards, Theoretical framework, Information ethics, Information searching.

INTRODUCTION

Widely available global information has brought with it both benefits and problems. Rather than describe any of the myriad of automated responses to breaches of academic integrity (or plagiarism) (as reported in (Joyce, 2007), for instance) the stance adopted in this paper is to go back to the fundamental nature of human information seeking (Bates, 2002). Bates suggests that there are we seek information in four main ways (Figure 3). These are: searching, which is active and direct; monitoring which is passive and direct; browsing, which is active and undirected; and being aware, which is passive and undirected. (Floridi, 2006) provides a starting point for this framework with his 'infosphere' (Figure 1) and levels of abstraction (Figure 2). (Wheatley & Frieze, 2006) have also informed the theorising for this framework with their theory and practice description concerning emergence. (Introna, 2005), in establishing multiple views of the nature of information technology when considering information ethics, is also considered in building the theoretical framework proposed below.

The structure of the paper is as follows: firstly the domain in which the theoretical framework applies is discussed; the theoretical framework is described; the next stage of the research project is proposed; and then implications for future research are discussed

RESEARCH DOMAIN

The domain chosen for the research proposed is a selection of Australasian academic literature reporting on research conducted on issues relating to plagiarism in computing. A framework based on seven basic tenets regarding information seeking and information reporting is described below (Table 1). From a preliminary literature review, the stance most commonly adopted appears to be that rules/guidelines are in place, have been taught to students and those who break these rules or guidelines will be punished. It also appears to be assumed that all academic writers should know how to perform correct writing and therefore will not plagiarise. Joyce (2007) suggests from his themed analyse of papers on academic integrity or plagiarism in the computing education literature that there is a lack of understanding about academic conventions ' . . .for which there is no single

remedy'. In adopting Bates (2002) theoretical positioning on searching it can be seen that there maybe many factors to consider in looking at academic integrity as a phenomenon.

A THEORETICAL FRAMEWORK FOR ACADEMIC INTEGRITY

The basic tenets underpinning this framework for academic integrity in computing are described below:

Basic Tenets

1. When academic integrity is explored as a subject of interest, there is an underlying moral or value judgement made. This moral or value judgement is that to claim the written work of others as your own is somehow wrong.
2. There are many stakeholders in academia: institutional managers; academic staff (who, in general carry out multiple duties including research, teaching and service); administrative staff; students; legal representation; industries supporting academic integrity (for instance, Turnitin.com); and academic funding agencies, both public and private. Stakeholder views may vary both within and between stakeholder groups. For institutional managers this usually means that policies and procedures are in place to manage academic integrity for both staff and students. Supporting industries may provide fee-for-service checking, monitoring, reporting and archiving of all submitted documents. Legal representation may be required for any of the above stakeholders if disputes arise.

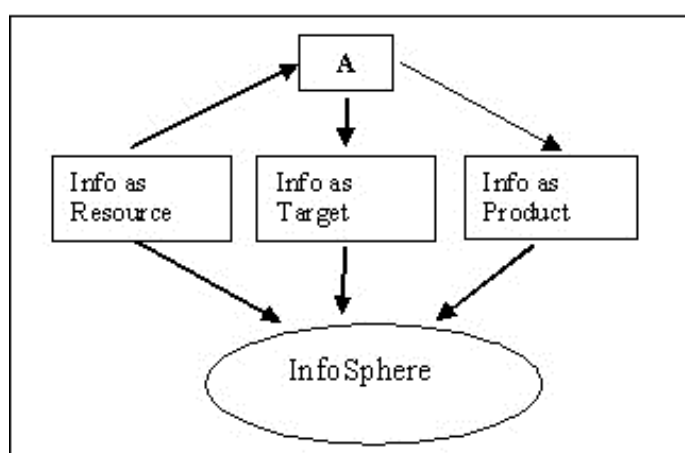


Figure 1: Infosphere (Floridi, 2006)

3. (Floridi, 2006) suggests that each player in an 'infosphere' will have a different level of abstraction (LOA). If we consider the 'infosphere' of academic integrity then each stakeholder is likely to have a series of LOAs which may or may not overlap. (Floridi, 2006) suggests that the 'infosphere' (Figure 2) is made up of information as resource, information as target and information as product. A typical process to produce an academic document based upon a research activity requires the following conditions to be met: a research project upon which the document is based; a literature review; a theoretical framework (which is often implicit rather than explicit); production of they research output; and the finished document. Floridi describes the literature review as information as resource, the process of writing as information as target and the finished product as information as product. It is important to note that the act of production involves the use of precise guidelines or rules on how to access and record the work of others. Maintaining academic integrity with respect to the research outputs of other writers means to follow these guidelines precisely.

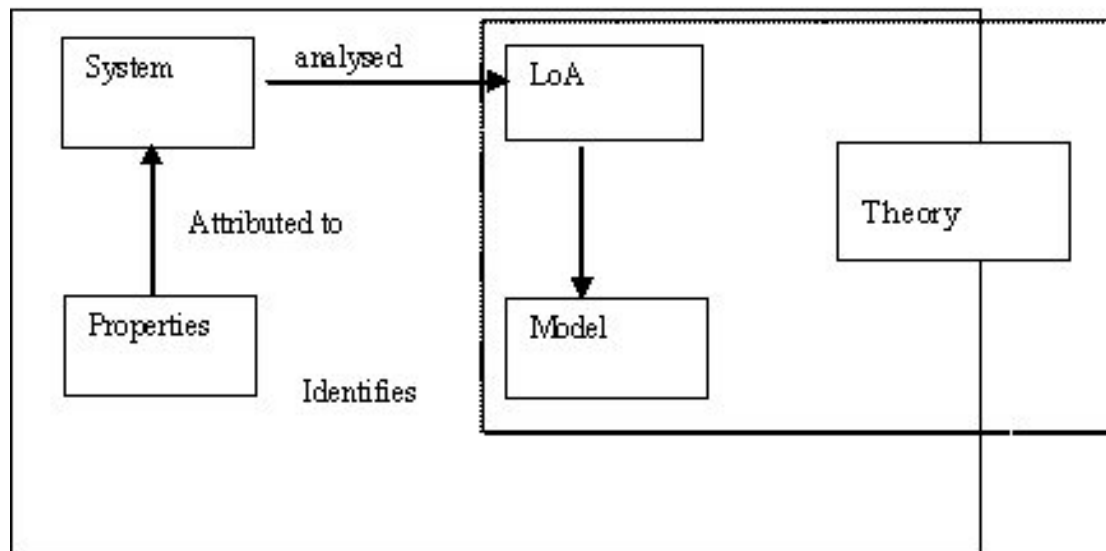


Figure 2. Levels of Abstraction (Floridi (2006))

4. Human information seeking (Bates, 2002) follows the path of least resistance. Bates suggests that we seek information in the following ways (Figure 3). Producing a literature review places the information seeker in the active/direct quadrant. Bates also suggests that of all the human information seeking behaviours, this is the least efficient. If a basic tenet of information seeking is that we find information in a daily living in the most opportune manner, then producing a literature review is counter to natural human behaviour. The question to be asked therefore is: because of natural human inclinations do we look for easy options in producing a literature review? Do these easy options include infringing the rights of others when using freely available written documents inappropriately (according to the rules of academic writing)?

	Active	Passive
Direct	Searching	Monitoring
Undirected	Browsing	Being aware

Figure 3: Bates (2002) Information Seeking

5. Introna (2005) suggests that information views about information technology may be broadly divided into 3 categories: Information technology as artefact or tool; information technology as social construction; and information technology as an ever-changing phenomenon. Introna (2005) suggests that when this stance is adopted an attempt is made to understand the subject in question (academic integrity (AI) in this case) and the impact this has on the community in which the impact is felt.
6. Academia operates within a global knowledge economy within a managed education climate (Boston, Mischewski & Smyth (2005). Implications arising from such a positioning are: an explosion in the number of academic research outputs being produced in most disciplines,

and in computing in particular; and many of these research outputs are freely available electronically.

7. In any economy when a product is available free of charge assumptions may be made about the worth of the item. Is there a link therefore between attitudes to what is available free of charge and how that free item may be used in the production of written academic outputs?

The Theoretical Framework

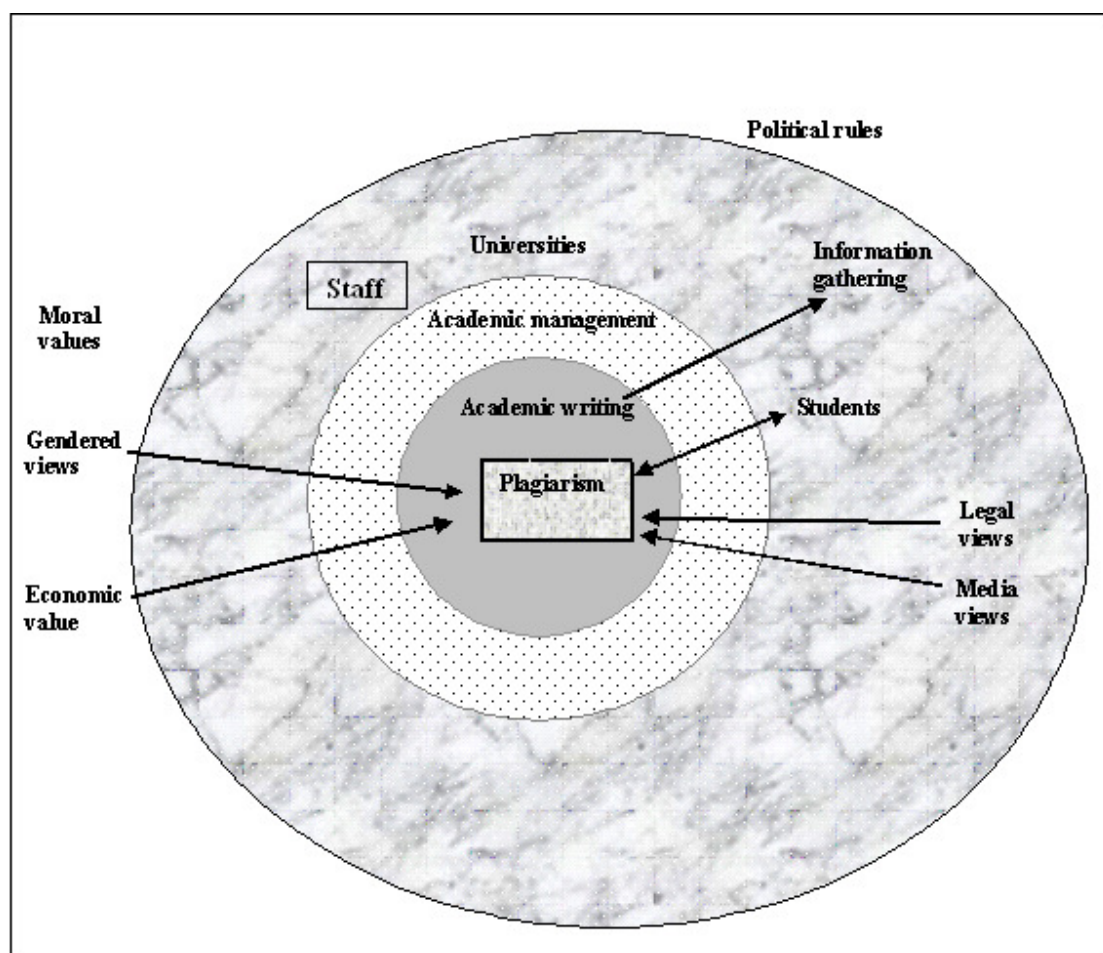


Figure 4 Stakeholder views and values

Figure 4 shows stakeholders, views and values incorporated in the proposed theoretical framework. In Table 1 shown below a model is proposed where stakeholders reporting on academic integrity are: academic staff, academic institutions, students, legal stakeholders, and media reporters. Basic tenet 5 incorporates Introna's (2005) categorisations of artefact or tool, social construction and phenomenology and is shown in Table 1 below as the categories chosen for analysis. It is also proposed that each of these three categories is further divided by gender. In collecting data it is proposed that papers from Australia and New Zealand be analysed.

It is expected that in analysing the selected literature on plagiarism that Floridi's (2006) notions on the 'infosphere' (Figure 1) will be applicable. Each paper reviewed will be evaluated for how information is treated – as resource, target or product – in the way in which plagiarism is discussed. The papers reviewed will also be evaluated for the level of abstraction, whether these levels overlap and to what extent.

View/Information	Artefact				Social				Phenomenology			
	C1		C2		C1		C2		C1		C2	
	F	M	F	M	F	M	F	M	F	M	F	M
Staff about												
Students, IT tools, institution, teaching practice, staff, theory												
Institution about												
Students, IT tools, managers, staff, teaching, plagiarism, rules												
Legal												
No hypothesised topics												
Media												
No hypothesised topics												
Student												
No hypothesised topics												
Note1: C1 = Country 1, C2 = Country 2 Note 2: author views on plagiarism will be recorded against each category Note 3: moral values recorded for each category Note 4: perceptions about information gathering will be recorded for each category Note 5: awareness of research value will be recorded for each category												

*Table 1 Academic Integrity reported in Computing
(Theoretical stance by author view of topic)*

Application of the Framework

The seven tenets proposed lead to the following set of hypotheses that will be tested in applying the theoretical framework.

Tenet 1 Moral and Value Judgements

The first hypothesis proposed is that:

H1. Authors adopt a moral stance on plagiarism or academic integrity.

When selecting the values to be tested against the framework, papers will be analysed for stated and un-stated moral or value judgements. These values will be recorded against each category in Table 1.

Tenet 2 Multiple Stakeholders

The second hypothesis proposed is:

H2. Academic teaching staff members are the dominant stakeholder group.

Scanning a selection of literature in the area of academic integrity or plagiarism suggests that the bulk of the writing originates with academic teaching staff members.

Tenet 2 forms the basis of stakeholder categorisation in Table 1.

Tenet 3 Influence of Dominant View

The third and fourth hypotheses proposed are:

H3. Rules and policies, practices, and assumed views will be influenced more by any particular dominant view.

The research proposed will test whether the dominant view influences the way in which academic integrity is reported. This hypothesis will be tested by analysing the results gathered from applying the framework shown in Table 1.

H4. There are gender differences in theoretical positioning adopted.

This research will test whether there are any gender differences in the way in which academic integrity is reported in the literature. Whilst this is not based on a stated tenet it is believed that there are gender differences in the way in which academic writers report on the issues associated with academic integrity. Hypothesis 4 will be tested by analysing the gender categorisation as shown in Table 1.

Tenet 4 Information Seeking

The fifth hypothesis proposed is:

H5. Authors are unaware of differences in the way in which information is gathered.

The research proposed will analyse the literature reviewed for stated or un-stated views on the manner in which information is gathered. This is at least a two-stage process. Subjects upon which plagiarism research is conducted will have information seeking behaviours as well as the researchers and writers. Hypothesis 5 will be tested by analysing results obtained from the recorded perceptions by categories in Table 1.

Tenet 5 Information Views

The sixth hypothesis is:

H6. Authors adopt at least one view of plagiarism in academic writing.

An author's view on academic integrity may be un-stated. This will be evaluated in the literature reviewed. Hypothesis 6 will be tested by analysing author views according to Introna's (2005) categorisation.

Tenet 6 Research Production in Managed Education

The seventh hypothesis proposed is:

H7. The production of academic writing and the precise rules and/or guidelines required to produce a research output with integrity influence writers' theoretical positioning.

It has been reported (for instance by Boston, Mischewski & Smyth, 2005) that political pressures brought about by a national measured academic research output system have had a number of effects on the way in which research is conducted and reported. There are claims that there is an explosion in the number of academic research outputs being produced, particularly in computing. This hypothesis will be tested by analysing the trends emerging from results obtained by applying the theoretical framework.

Other authors also suggest that such a rating scheme adds 'noise' to the quantity of research outputs available without improving the overall standard of research. This is marked contrast to Boyer's (1990) views on the cornerstones of academia being scholarships of discovery, integration, application and

teaching. (The scholarship of discovery is most recognizable as "research," the search for knowledge for its own sake, and the principled mode of inquiry that characterizes this quest.

A knowledge economy measured output scenario tends to favour short-term, pressured returns that do not encompass the higher levels of reflection (Bain et al, 1999) necessary and ones that mature with thoughtful research and scholarship. This view will be tested when the framework is applied to a body of computing literature written within the 1999-2006 period - the current 'knowledge economy' with measured outputs.

Tenet 7 Freely Available Research Outputs

The eighth hypothesis is:

H8. Research outputs available free of charge devalue the content.

In any economy when a product is available free of charge (which appears to be the case in a globally – connected virtual world) assumptions may be made about the worth of the item. The link between attitudes to what is available free of charge and how that free item may be used in the production of written academic outputs will be tested. Awareness of research value will be recorded in each category in Table 1 in order to test the eighth hypothesis.

FURTHER RESEARCH

Further research to apply this theoretical framework to a body of computing literature in academic integrity is the subject of another paper. A collection of 130 Australasian papers published in this field are currently being analysed according to the framework proposed. Early results suggest that a mechanistic view is adopted by a majority of authors and that the phenomenon of plagiarism is treated as an artefact. Very few authors adopt any deeper philosophical stance or consider plagiarism in the light of a wider social construct.

It is expected that when results are analysed Wheatley and Frieze's (2005) emergence concepts will be applicable.

A theoretical framework that provides a deeper philosophical approach to plagiarism, information seeking, levels of abstraction in theorising about academic integrity and the acceptance of multiple points of view has the potential to both broaden and deepen the collected wisdom on what is understood by academic integrity.

CONCLUSION

In this paper a theoretical framework is proposed with which to gain a deeper understanding of global positioning adopted with respect to academic integrity. Whilst it is proposed that the basic tenets be tested on the Australasian literature on academic integrity, it is also appropriate to apply the framework to a larger international sample.

REFERENCES

Bain, J.D., Ballantyne R., Packer, J., Mills, C. (1999). Using journal writing to enhance student teachers' reflectivity during field experience placement. *Teachers and Teaching: Theory and Practice*, 5(1), 51-73.

Bates, M. (2002). Toward an integrated model of information seeking and searching, *The New Review of Information Behaviour Research*, 3, 1-15.
http://www.gseis.ucla.edu/faculty/bates/articles/info_SeekSearch-i-030329.html accessed 10 January, 2008.

Boston, J., Mischewski, B., & Smyth, R. (2005). Performance - Based Research Fund - Implications for Research in the Social Sciences and Social Policy. Social Policy Journal of New Zealand, 24, April. <http://www.msd.govt.nz/publications/journal/24-April-2005/index.html> accessed 14 January 2008.

Boyer, E. L. (1990). Scholarship Reconsidered: Priorities of the Professoriate San Francisco: Jossey-Bass.

Floridi, L. (2006). Information ethics, its nature and scope. SIGCAS Computers and Society, 36(3), 21-34.

Introna, L. (2005). Phenomenological approaches to ethics and information seeking, Stanford Encyclopaedia of Philosophy. [plato..stanford.edu/entries/ethics-it-phenomenology/](http://plato.stanford.edu/entries/ethics-it-phenomenology/) accessed 31 May 2007.

Joyce, D. (2007). Academic Integrity and Plagiarism: Australasian Perspectives. Computer Science Education Australasian Special Issue. Accepted 31 May 2007, XX(X), XX-YY.

Wheatley, M., & Frieze, D. (2006). Using emergence to take social innovations to scale. <http://www.margaretwheatley.com/articles/emergence.html> accessed 14 January 2008.

COPYRIGHT

[Kay Fielden] ©2008 The author(s) assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

Scandal, Censorship and Representation in the Online World: An Ethical Conundrum

Graeme Pye¹

Alyson Miller²

¹School of Information Systems, Faculty of Business and Law

²School of Communication and Creative Arts, Faculty of Arts and Education

Deakin University

Geelong, Australia

Email: graeme@deakin.edu.au and amil@deakin.edu.au

Abstract

This research begins by examining the foundation issues of content censorship from a literary perspective and then proceeds in comparison to discuss the issues of online content appropriateness and whether the same censorship principles of literature are transitional to the online world. Currently, uncertainty exists in how to tackle this issue as there appears to be a lack of formal rules or suggested guidelines applied to the content appropriateness, management and availability of online material. Therefore, where does the onus of online content censorship exist in this medium? Or is it left to the ethical and moral standards of the material source/creator, online access provider or the cultural ethics of the wider community to adjudicate?

Keywords

Literature, online censorship, ethics, publication.

INTRODUCTION

Recent media reports regarding the posting of adverse incidents and materials on the Internet continues to call into question the controls concerning the nature, content and substance of data placed online, and the ease with which such postings can be made public. There has been somewhat of a community scandal regarding the types of incidents depicted, combined with an outcry concerned with a perceived lack of censorship and ethical judgement regarding the ease with which such online representations are publicly accessible via the Internet.

Prior to the availability of online self-publication, the issue of material censorship was initially based in literature, and with the progressive development of technology, increasingly extended to cross-media broadcasting (i.e. radio and television), films and computer games. The freedom and lack of rules or guidelines in the online world has opened a new and complex dimension in the censorship debate, furthering difficulties about the nature of representation and the influence it maintains over the consumer. The boom in online pornography for example, has proved particularly volatile, raising questions regarding obscenity, morality and the notion that access to certain types of representation is capable of causing subjective harm. The issue of controlling online matter is particularly pertinent when discussing the nature of pornographic depictions and the relative ease with which such material is accessible and is a clear example of the ethical dilemmas associated with Internet usage.

TRADITIONAL LITERATURE AND CENSORSHIP

Australia enforces a classification system upon films, magazines and computer games before their public release; however when it comes to matters of the literary, censorship and censoriousness often centre on subjective questions of taste, on aesthetic judgements of artistic quality, and on debates concerning the functionality of literature in public and private spheres. Literature and censorship have enjoyed a long and antagonistic relationship, particularly during the late nineteenth and early twentieth centuries, with the likes of Charles Baudelaire, Gustav Flaubert, James Joyce, D.H. Lawrence and Vladimir Nabokov. In each of these cases, debates were fuelled by socio-cultural expectations

regarding gender and sexuality, blasphemy and moral norms, and underpinned by the premise that the relationship between word and world, representation and action, was performative, that material depicted could (and would) effect behaviours enacted.

While literature now appears to be a dying cultural form in a society centred on the hype of graphic media, the power of the word to unsettle remains a remarkably frequent phenomenon. In the past 20 years, texts such as Salman Rushdie's *The Satanic Verses* and Bret Easton Ellis' *American Psycho* have inspired a gamut of anxieties concerning the transformative nature of representation, the transgressive qualities of text and the potentially 'harmful' influence of consuming 'morally ambiguous' fictions. *The Satanic Verses* has had a particularly hyperbolic history, causing international upset due to Rushdie's unfavourable interpretations of the Koran and ostensibly heretical comments upon the Islamic faith. As Daniel Pipes (1990) observes, it engaged thousands of individuals in protest, "caused the deaths of over twenty people, disrupted billions of dollars in trade, brought profound cultural tensions to the surface and raised issues about freedom of speech and the secular state that had seemingly been settled decades or even centuries earlier" (p. 16). More recent examples include the notoriety of *The Da Vinci Code* (2003), an astoundingly popular success that nonetheless provoked outrage in the Catholic Church and scandal regarding Dan Brown's claims that the novel was truth-based and his supposed plagiarism of *Holy Blood, Holy Grail*. Kathryn Harrison's memoir *The Kiss* (1998) attracted enormous attention on its public release, given its telling of an incestuous relationship between the 20-year old Harrison and her estranged father. It was the object of debates concerning *representability* – what should and should not be depicted, regardless of artfulness – and the idea that transgressing cultural taboos has now become a marketing tool for fame and profit.

The ambiguity often attached to literature as a cultural medium has ensured that difficult material has a history of misunderstanding and misreading. Flaubert's *Madame Bovary*, for example, charged with depraving public morals in its depiction of Emma Bovary's adultery, is an ironic denunciation of the self-satisfying delusions of the bourgeoisie. Lawrence's *Lady Chatterley*, condemned for its sexual permissiveness and rejection of traditional family morals, is in fact rigidly patriarchal. *American Psycho*, with its brutal and graphic series of the violent rape and dismemberment of countless women, and its murderous destruction of homosexuals, ethnic minorities, the homeless and various animals, is an unrelenting critique of dominant phallogentric, materialist, misogynistic, white middle-class male culture. Yet the willingness to misconstrue text in order to promote its censorship, or to advocate public censoriousness, is far from random. The continuity lies in the capacity of scandalous texts to critique the status quo, to trouble cultural norms and boundaries. The imperative behind literary censorship, then, can be seen as an ideological drive seeking to maintain normative paradigms, to control the nature of representation in order to control socio-cultural, religious and political mores. The notion of ethical propriety can thus become little more than protecting the interests of potentially outdated, unjust and oppressive modes of hegemonic power. The irony, of course, is when texts such as *American Psycho* attract vitriolic censoriousness: read superficially, it hyperbolically endorses the norms of mainstream culture whilst read analytically, it supports the political agendas of feminism, refutes the excesses of materialist consumerism and highlights the destructive stereotypes attached to those at the ethnic margins.

Arguably, then, censorship in literature is predicated on critical reading, on ascertaining a fixed meaning from a text and designating its normative/transgressive qualities. Split between an ethos of public information and public entertainment, the novel is a slippery mode, bordering on subjective modes of interpretation and analysis in order to assign a set of possible meanings among a myriad of other likely explanations. Yet in terms of the potential for scandal, literature is a medium that seems oddly orchestrated. Given the long processes of review that a manuscript is subjected to before it is publicly censured, there are imperatives behind scandalous texts that are missing from the instantaneity of the Internet. The novel is a carefully managed product, not the result of a whim and because of this, tends to carry the weight of greater socio-cultural, political or religious initiatives. That is, literary scandal and the scandal of offensive on-line material differ fundamentally in terms of time distancing, the space between the production of a form and its release for public consumption. The result is that literary texts often possess a form of shock-value that contains deeper ideological (social, political, cultural, etc.) agendas; the transience and transformability of the Internet, however, often seems to evade the careful management offered by the literary process.

Yet like the Internet, the novel has always been involved in blurring the gap between spheres, in exposing the private to public scrutiny (Morrison & Watkins, 2007, p. 4). The Internet, however, has

taken the breach between spheres to a whole new level; to the extent, in fact, that the notion of 'private' has become an ideal for those 'too repressed' to join FaceBook, create an online Blog, remain logged in to MSN, or divulge all on a MySpace profile. While literature retains the imperative of fictionality and requires, to some extent, the patience of concentrated reading and some degree of analytical thinking, the Internet is a medium that allows not only all-welcome access, but also free-range contribution. Thus while literature is subjected to the difficulties of publication acceptance, editorial judgements and critical review, the Internet is a source seemingly void of parameters and as such, theoretically limitless in its content.

However, the Internet, like literature, is highly subject to the censure of public viewing, to the reactions of an audience critical of the material it accesses for either educative or entertainment purposes. The difficulty, of course, arises in the very nature of the Internet: it is a free-for-all medium, instantaneous, user-friendly, endless in its capacity and lacking in parameters, imagination, desire and technical knowledge often the only impediments to its manipulation. And whilst legality ought to prevent the worst of its excesses—child pornography, for example—the Internet remains a place seemingly devoid of restrictions capable of protecting the public from demoralising, unethical and, arguably, 'harmful' representations posted by unscrupulous users.

A recent example of this lack of online editorial judgement that drew considerable media attention was the reaction to a video posted on the self-broadcasting community website, YouTube. This was a video of an incident at a Skate Park involving a vicious physical assault on a ten year old boy and depicted the victim being struck repeatedly, while another scene of the video shows a group of older children surrounding and taunting this same individual until he lashed out. A witness to the incident used a mobile device to film this assault, which was subsequently publicised on the YouTube website. The news media reporting and the ensuing public outcry by the community resulted in removal of the offending and the police pursuing further investigations (Breen 2007).

This video is a clear example of digital exhibitionism and exemplifies how the freedom of the Internet and the associated technologies can be utilised for self-publication purposes without the material content necessarily subjected to the rigour of critical editorial review, censorship or any ethical criteria whatsoever, until after the community reaction and complaint. In defense of YouTube™, they obviously cannot monitor or review every video uploaded to their website and therefore largely rely on the ethics of the users in making judgements prior to posting. The YouTube Community Guidelines provide a layman's version focusing on certain common sense rules in lieu of the legalistic detail contained in the 'Terms of Use' document. These guidelines essentially ask YouTube users to apply and consider the appropriateness of the material content prior to posting online and are listed as follows (YouTube 2007):

- YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement and we report child exploitation. Please read our Safety Tips and stay safe on YouTube.
- Don't post videos showing bad stuff like animal abuse, drug abuse, or bomb making.
- Graphic or gratuitous violence is not allowed. If your video shows someone getting hurt, attacked, or humiliated, don't post it.
- YouTube is not a shock site. Don't post gross-out videos of accidents, dead bodies and similar things.
- Respect copyright. Only upload videos that you made or that you have obtained the rights to use. This means don't upload videos you didn't make, or use content in your videos that someone else owns the copyright to, such as music tracks, snippets of copyrighted programs, or videos made by other users, without their permission. Read our Copyright Tips for more information.
- We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech, which is content intended to attack or demean a particular gender, sexual orientation, race, religion, ethnic origin, veteran status, colour, age, disability or nationality.

- There is zero tolerance for predatory behaviour, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information. Anyone caught doing these things may be permanently banned from YouTube.
- Everyone hates spam. Do not create misleading descriptions, tags, titles or thumbnails in order to increase views. Promoting your channel is one thing, but it's not okay to post large amounts of untargeted, unwanted or repetitive content, including comments and private messages.

YouTube is ubiquitous and accessible to users of all ages with differing cultural and contextual interpretations of the materials posted online. From this perspective it is evident that YouTube is chiefly concerned with the legal perspectives of free speech, copyright and tolerance and yet provides little ethical guidance to the user regarding the censorship of inappropriate content, thus relaying on the perception that people generally will act ethically of their volition. Obviously, not all users would even read these guidelines, let alone the 'Terms of Use' document and therefore cannot be a reliable means of content management or guide for ethical user behaviour. Invariably, the reaction is to use technology to automatically addressing content management issues.

TECHNOLOGY-BASED ONLINE CENSORSHIP

A specific example of the technology-based censorship was YouTube's management of the unauthorised or pirated copyright materials appearing on their website. YouTube itself implemented content filtering technology to automatically identify and remove copyrighted materials previously identified by the copyright owners as a move to placate the movie and television studios, particularly in lieu of a \$1.1 billion content piracy suit bought by Viacom in the United States (Anon 2007a).

Another example of censoring online material content now exists in 1600 Victorian State Schools through a ban that denies student access to video-sharing websites such as YouTube in order to limit the growing occurrence of cyber-bullying. This action utilises filtering technology based on text and blocking access of websites as identified by the Education Department such as YouTube and MySpace (Smith 2007).

No-one would argue that the protection of minors from access to unsuitable online content requires some form of censorship and remains an ethical obligation of governing bodies. As the previous YouTube example alludes to, this technology enables self-expression and exploitation of almost instantaneous publication and yet there is no space for editorial consideration prior to publication, unlike traditional literature. Therefore, once an ill-considered piece is publicly online, it becomes irretrievable and open to all types of moral interpretations.

These examples serve to illustrate the instantaneous nature of the online medium that now has authorities grappling with how to address and develop means of managing the content accessibility and censorship of Internet material.

FEDERAL GOVERNMENT ONLINE CENSORSHIP

Currently this area is in a state of flux, but the previous Federal Liberal Government focused their online content censorship efforts on specifically safe Internet use for children by utilising and providing filtering software options for parents to install on their home computers as a means of blocking children from inappropriate online material content and engaging in undesirable activities and behaviours. The thrust of the Australian Government's online safety program NetAlert is the program's website freely providing educational and guiding information for parents, teachers and librarians across a number of areas including, but not confined to (NetAlert 2007):

- Cyber bullying;
- Cyber stalking;
- Supervising children online;
- Online publishing;
- Paedophiles and pornography;
- Online safety tips for adults, teenagers and children;

- Spam, and
- Staying safe in online chat rooms.

This represents a starting point with an educational and preventative focus but is not a complete online censorship solution and with the change in federal government, NetAlert's future is uncertain. An alternative method of online censorship is the introduction in January 2008 of access restrictions to online chatrooms and websites imposed upon those companies that sell entertainment-related content via Internet subscription. This will now compel providers for the first time to check that people accessing MA15-plus content are indeed over 15 years of age and those accessing R18-plus or X18-plus are over 18 years of age (Anon 2007b). The enforcement of these provisions falls under the auspice of the Australian Communications and Media Authority (ACMA) who are responsible for monitoring internet content, enforcing Australia's anti-spam laws and making rules in regard to accessing the Internet. In this case the ACMA will be able to compel content providers: to remove offensive material, issue notices for live streaming content to cease and the removal of web links to offensive content (ACMA 2007).

Furthermore, current Federal Labor Government policy and legislation would compel ISP's (Internet Service Provider) to supply a 'clean feed' by filtering and blocking access to the ACMA's non-approved website 'blacklist' for all customers and schools, which amounts to nothing more than government censorship by stealth. Of course the policy would enable people to opt-out of the service by contacting their ISP for uncensored access (Dunlevy 2008) however; this should not be the default position.

Arguing for child protection in order to censor online access and viewing choices for adults is not the answer and deeper consideration identifies numerous technical, financial, moral and social difficulties with implementing this policy (English 2008). As Clarke (2007) noted of the previous government's policy, this enables the use of indiscriminate draconian powers and should not be the right of any democratically elected government. Adults and parents should be free to make their own judgements regarding Internet content censorship and take an active interest in their children's online activities and utilise freely available filtering software and advice to control their online viewing habits, if they choose. Moreover, the question of 'accessibility' is one often placed in hyperbolic terms, suggesting that ethically ambiguous sites and postings are simply 'there', lying in wait to spring upon an unsuspecting user as they browse. Like plastic-wrapped magazines and censored texts, unethical on-line material is something that has to be consciously looked for, or even bought; it is unlikely, for example, that whilst conducting a search for statistical data the user finds themselves regaled by a series of child pornography. Thus while 'harmful' representations clearly abound, the notion of discovery is complicated by the idea of wilful desire, and the right of a consenting adult to access (within the parameters of the law) content freely.

THE ETHICAL CONUNDRUM: WHAT ETHICAL APPROACH TO TAKE?

To address effectively the ethical conundrum of online censorship there is an evident requirement to broaden of scope away from just the narrow technological solution option, to one that encompasses a review of the traditional literary censorship debate, seeks to develop wider and inclusive education programs and taking into consideration the ethical and moral components of censorship under the following non-exclusive overarching points as listed:

- Like literature, on-line censorship should be self-initiated, instigated by the moral positioning and ethical standpoints of the individual;
- Offensive material is a subjective viewpoint; however, some forms are simply illegal and thus subject to legal ramifications;
- The notion of the 'ethically publishable' is a continuation of old literary debates; however it has failed to transfer into the realm of new technology. So the processes of review that literature is subjected to no longer stand; the Internet is a medium of immediacy, and lacks the objective time distancing associated with hard-copy published forms;

Current approaches to manage Internet material content remains at the periphery of the issue by only utilising technological means for compliance enforcement and content-blocking. There remains a need to broaden the search for answers to this problem and reflecting on the literature's dealing with and

managing of the material content offers insight into the subjective area of censorship. Unlike literature, where the content is open to interpretation and analysis, here the online medium presents material instantaneously to the viewer, who is therefore at the mercy of the ethical beliefs of the source regarding content suitability. Nevertheless, to suggest that the Internet should be fitted with censorial systems' adjudicating the nature of material accessed is to suggest that an individual is incapable of determining a subjective response that adequately deals with that content. That is, a user offended by perceived unethical representation is capable of rejecting that representation without the assistance of a 'nanny over-seer', able to log-out, to lodge complaints, to refuse to support the nature of the material available. A user is able to reply and react to offensive material intelligently without the manifestation of Big Brother superstructures determining the nature of response.

CONCLUSION

Literature enables the reader to inhabit the character and yet apply their own ethical beliefs or at least understand through analysis the textual meaning of the literary piece and then choose whether to adopt, argue or reject the premise. Whilst the notion of a reader 'inhabiting' a character has been the cause of considerable debate and controversy (Ted Bundy, for example, notoriously claimed that *American Psycho* compelled him to rape, murder and dismember women, as Wade Frankum similarly credited his Sydney killing spree to his love for the text), literary works are subjected to rigorous pre-release judgements that mitigate the instantaneity associated with nefarious on-line content. On-line, you are immediately subject to overriding visual content and its specific perspective, and are therefore at the ethical mercy of the 'poster'. Whilst this is not to suggest that literature does not represent the unethical (clearly a misnomer), the immediacy granted by the Internet—the immediacy of uploading, downloading, updating and transforming—proves problematic for the nature of the scandal it is capable of causing; scandal that is capable, as evidenced by cases of cyber-bullying, paedophilia, on-line stalking and child pornography, of actual harm.

Whatever governments do is only playing at the fringe in order to placate community concern, the result being an ad hoc approach that is neither effective nor systematic. Education is the key, where the freedom to consume ought to remain the fundamental principle of access and default position, not the 'nanny' state version that attempts to regulate the minds and thoughts of individuals via governmental ethos driven censorship principles. Inarguably, some forms of representation are simply illegal (e.g. child pornography), thus the notion of censoring select content is a moot point in the ethical debate.

There will always be digital exhibitionism and adults should remain free to choose, apprise and decide what content they wish to view regardless of imposed censorship limitations. Additionally, adopting universal ethical guidelines would help, if only to inform that choice and protect those who wish—and need—protection.

REFERENCES

- ACMA 2007, *Restricted Access Systems Declaration 2007*, [Online], Australian communications and Media Authority, URL: <http://www.acma.gov.au/WEB/STANDARD/pc=PC_310905> Assessed: <January 2008>.
- Anon. 2007a, 'YouTube goes into damage control.' *Geelong Advertiser*, Geelong, Daily, 17 October 2007, pp. 22.
- Anon 2007b, 'Web limits for kids', *Herald Sun*, Melbourne, First, 22 December 2007, pp. 18.
- Breen D. 2007, 'Police to quiz mob involved in vicious skate park attack Bullies exposed', *Geelong Advertiser*, Geelong, Daily, 23 November 2007, pp. 4.
- Clarke R. 2007, *Media Release: Internet Censorship Bill*, [Online], Australian Privacy Foundation, URL: <<http://www.privacy.org.au>> Assessed: <January 2008>.
- Dunlevy S. 2008, *Rudd online porn-free plan questioned*, [Online], The Australian, URL: <<http://www.australianit.news.au>> Assessed: <January 2008>.
- English G. 2008, *Labor online strategy slammed*, [Online], The Australian, URL: <<http://www.australianit.news.com.au>> Assessed: <January 2008>.
- Morrison J. & Watkins, S. (eds), 2007, *Scandalous Fictions: The Twentieth-Century Novel in the Public Sphere*, Palgrave Macmillan, Basingstoke.

- NetAlert 2007, *Protecting Australian Families Online*, [Online], Attorney-Generals Department URL: <<http://www.netaalert.gov.au>> Assessed: <December 2007>.
- Pipes, D. 1990, *The Rushdie Affair: The Novel, the Ayatollah and the West*, Carol Publishing, New York.
- Smith B. 2007, 'Schools ban YouTube sites in cyber-bully fight', *The Age*, Melbourne, First, 2 March 2007, pp. 5.
- YouTube 2007, *YouTube Community Guidelines*, [Online], YouTube, LLC, URL: <http://www.youtube.com/t/community_guidelines> Assessed: <December 2007>.

COPYRIGHT

Pye and Miller ©2008 The author(s) assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

Virtual World, Real Ethics: Challenges for Online Counselling

Rebecca Andary¹
David A Banks²

¹Relationships Australia (SA)
Adelaide, Australia

Email: r.andary@rasa.org.au

²School of Computer and Information Science
University of South Australia
Adelaide, Australia

Email: david.banks@unisa.edu.au

Abstract

The demand for counselling services continues to grow around the world and responses by counselling organisations to provide support for a larger and geographically spread client base have led to the adoption of new online technologies. Standard technologies such as email and chat have been introduced to support specific counselling situations but increasingly attention is turning to online social networking and virtual world environments as vehicles for supporting more diverse counsellor-client interactions. This paper explores the potential ethical problems that arise when social networking systems such as Second Life are considered as vehicles for supporting counselling.

Keywords: Counselling, virtual environments, Second Life, avatars, ethics.

INTRODUCTION

The Internet has fast become integrated into our day-to-day lives as an information resource, communication tool and as an alternative to accessing and purchasing goods (Ybarra & Eaton 2005; Mesch & Talmud 2006). It is not surprising then that consumers are also looking to the Web for the purchasing and receiving of services such as online counselling. Further, the trend now developing is the navigation towards 'customizable digital [media]' (Williams 2006, p. 69) such as the virtual world, Second Life. Second Life differentiates itself from online computer games as it is a natural progression from the real world and is free of the structure that governs online computer games. As such Second Life becomes a viable possibility as a platform for the enactment of online counselling. Before considering the place of social networking systems such as Second Life we outline the broad aims of counselling and consider the ways that technology is already being used.

COUNSELLING

It is important at this stage to identify what is meant by the term 'counselling'. In order to define counselling it is useful to consider the reasons why people seek counselling and what they hope to achieve through it (Geldard & Geldard 2001; Egan 2002). Generally speaking, people seek help when they are emotionally troubled, are experiencing a crisis or are feeling emotionally vulnerable and 'believe they are unable to solve their problems and resolve their distress without outside help' (Geldard & Geldard 2001, p.4). The goal of counselling is therefore to empower clients with the skills and knowledge to utilise the resources available to them and manage their current and future situations more effectively (Egan 2002).

For the purposes of this paper, the term 'counsellor' includes psychologists, social workers, counsellors, and any other professional offering a mental health therapy service. Counsellors are trained to deal with clients in face-to-face situations and are guided in their dealings with clients by well recognized professional codes of ethics, for example the Australian Psychology Society's Code of Ethics provides guidelines for psychological assessment procedures and relationships with clients.

There are also underlying counselling models that can be used to provide a guiding framework for the counselling process. Egan's Skilled Helper Model (Egan, 2002) for example offers "a problem-management and opportunity-development approach to helping" (Egan 2002, p. 24). Its three stages are about assisting the client to find out what is going on in their lives, what solutions are available and how they might achieve their needs or wants.

This model provides a great deal of flexibility and is about empowering the client with the problem solving skills to help them solve their problems. In an earlier book Egan noted that The skills of the human helper are paramount and develop from appropriate training and life experiences of the counselor and Egan notes that "The trainee [counselor] should own the model, not be owned by it. He eventually must call upon all available resources – his own experience, other systems and technologies, research, developing theories – to clarify, modify, refine, and expand the model." (Egan, 1975, p.50) This emphasises the dynamic and adaptive aspects of counselling. The advent of new online environments will require counselors to develop new models and approaches, or adapt existing ones, if they are to provide appropriate and ethical support for their clients.

GROWING DEMAND AND THE ROLE OF TECHNOLOGY

The Victorian Department of Human Services released a publication in 2002 highlighting that the number of clients seeking mental health services increased by 24% from 1997-98 to 2000-01 (State of Victoria, Department of Health Services 2002, p.6) and this increase in the demand for counselling services is not isolated to Victoria. Relationships Australia (SA) has also seen a steady increase in the demand for counselling over the past six years. They have continued to provide counselling to a steady number of clients but have seen an increase in the number of clients on their waiting list resulting in a jump from a 6-8 week waiting time in 2005 to a 2-5 month waiting time in 2007.

Given this increase in demand for counselling services, and the finite number of counsellors and counselling resources available there is a clear need for an alternative method of service delivery to provide both efficiency and efficacy. Computer technology has already been used to provide support for traditional face-to-face counselling practice, for example in family law (Belluci and Zeleznikow, 2001), and in areas of sensitive family problems (Fielden and Goldson, 2006). In these situations the technology is used essentially as a mediating tool to support traditional face-to-face counselling and would not appear to raise any significant new issues in terms of ethics. Online counselling, however, is an alternate method that will increasingly be utilised in the future it is imperative that the problems associated with this are understood.

ONLINE COUNSELLING AND ETHICS

In response to these growing demands for counselling services internet-based technology has been seen as a possible way to provide additional communication channels to reach clients. In a society where there is a stigma around seeking counselling and where counselling is often perceived as a sign of weakness clients themselves are also turning to the internet (Geldard & Geldard 2001). In addition to the lack of need for revelation of personal problems outside a limited communication channel, access issues such as time and location provide compelling reasons for individuals to turn toward the internet for help (Palaniappan & Jun-E 2006). Research suggests that around twenty-five percent of young people and "twenty-six percent of adult Internet users have searched for information about mental illness" (Ybarra & Eaton 2005, p.75) with the primary reasons cited being convenience and anonymity (Christensen & Griffiths 2002; Palaniappan & Jun-E 2006).

All counselling service delivery methods require recognition of ethical issues, and psychological, counselling and social worker associations in countries such as America and Australia have established a code of ethics that their members must follow in order to limit these risks. Nonmaleficence, or 'Do No Harm', is perhaps the most common ethic associated with medical and health care professions and in the American Psychological Associations (APA) Code of Ethics this is the first general principle. The APA clearly states that "Psychologists strive to benefit those with whom they work and take care to do no harm. In their professional actions, psychologists seek to safeguard the welfare and rights of those with whom they interact professionally..." (American Psychological Association 2002, p.3). Online counselling enhances the risks associated with traditional counselling methods and allows for the emergence of risks not present in traditional counselling methods (Childress 2000). Online counselling services are currently available through many websites and in 1999 the American Psychological Association (APA) recognised the growing popularity and significance of these services and released a document entitled *Ethical Standards for Internet Online*

Counselling (Chester & Glass 2006). Many other countries, including Britain, Canada and Australia have since followed the APA's lead and released their own guidelines for online counselling. In recent times this code of ethics has been extended to the encompass delivery of online services (Chester & Glass 2006).

OPPORTUNITIES ARISING FROM ONLINE COUNSELLING

Currently online counselling services are primarily email and real time chat based. This is a relatively new area and Chester & Glass (2006) note that there is limited literature reviewing online counselling effectiveness and the few studies available are based on services in America. The literature that is available suggests that relationships and depression are the two problem areas people most frequently seek online counselling for (Chester & Glass 2006; Ybarra & Eaton, 2005). Interestingly, in an online environment people seem more willing to respond truthfully and "cut to the chase" of the core issues" (Rochlen, Zack & Speyer 2004, p.269) and 'self-disclose a greater degree of sensitive information online compared to in person' (Ybarra & Eaton 2005, p.77). Rochlen, Zack and Speyer (2004) suggest that the text-based interaction facilitates the rapid development of intimacy and honesty between the client and counsellor. Online counselling can offer benefits for both client and counsellor, as summarized below:

- Reaches those living in remote areas,
- Accessible to those with disabilities, immobilising illnesses, the elderly, and those confined to their homes,
- Convenient,
- Anonymous,
- Decreases defensiveness,
- Rapid development of trusting relationship between client and counsellor.

CHALLENGES ARISING FROM ONLINE COUNSELLING

Despite the potential benefits that can be obtained from online counselling, there are a number of disadvantages, particularly for the counsellor. Online counselling removes many of the verbal and non verbal cues that help the counsellor gauge the mood and reactions of the client during the counselling process. For the counsellor, non-verbal cues often provide useful signals about the client's emotional status and often assist the counsellor in assessing the client and making a diagnosis (Childress 2000). Counsellors also use non-verbal cues to show empathy and support which foster the client counsellor relationship and 'enhance the counselling process' (Geldard & Geldard, 2001, p.35-39). Non-verbal cues include physical closeness, the use of movement, facial expressions, eye contact, use of voice, and the use of silence (Geldard & Geldard 2001). Often in times of stress what we say and what we mean are different but 'our nonverbal behavior has a way of "leaking" messages about what we really mean' (Egan 2002, p. 84) and, particularly for clients who are defensive and slow to open up, non-verbal cues significantly aid the counselling process (Egan 2002). The absence of non-verbal cues can also increase the chances for miscommunication which can inadvertently harm or cause unnecessary trauma to the client (Childress 2000). Miscommunication in face-to-face counselling can easily be recognised through non-verbal cues such as retraction, and looks of shock and can quickly be corrected. In online communication environments it can often be undetected (Childress 2000), leading to the risk that the dejected client will terminate the counselling session and disappear into the virtual realm. Counsellors will need to be trained in online counselling communication skills to reduce the risks of miscommunication.

In addition to the challenges of the traditional counsellor's skills in this new environment, other concerns arise including limitations to crisis intervention, potential problems due to unperceived cultural differences, and concerns about identity verification and security (Rochlen, Zack & Speyer 2004). Equally, some clients may not have the skills, confidence or finance to allow them access to the technology and this leads to a situation where equity of access to the service is compromised. These concerns all give rise to significant ethical concerns.

Despite the loss of some cues in online counselling using email and chat facilities a skilled counsellor can include some social cues in their communications, for example by means of emoticons and carefully crafted language. However, the potential adoption of newer communication channels that are emerging in the Web2.0 environment poses an even more challenging set of problems for counsellors.

COUNSELLING IN VIRTUAL WORLD ENVIRONMENTS

It is clear that online counselling using email and chat systems can provide benefits but also raise a number of difficulties. In this next section of the paper we consider the issues surrounding the extension of counselling into virtual environments, particularly Second Life. Virtual communities have been around for decades and are well documented by authors such as Howard Rheingold. However virtual communities have evolved over time from the purely text-based chat room and email virtual community, through Whole Earth 'Lectronic Link (WELL) that Rheingold joined in 1985 (Rheingold 1993), to the current day 3D graphics described as Massively Multi-Player Online Games (MMOG). These are essentially gaming environments with specific goal-oriented drivers and are populated by individuals or teams of players. The players in these MMOGs take on a persona as part of the game playing. Another large system where individuals take on a persona, or avatar, is known as Second Life. Second Life, like other virtual communities throughout time, allows people to concurrently live multiple personas often with different genders (Danet 1998; Rheingold 1993). Unlike the MMOGs, Second Life is a virtual world that has an online society that resembles the 'real' world. That is to say, there is no gaming intent pervading the world and individuals, representing themselves through avatars, are free to roam the domain and interact in a limited way with objects and other avatars. Rheingold (1993) believes that computers and "computer-mediated communications media seem to dissolve the boundaries of identity" (Rheingold 1993, p.147). Further the relationships people build within these virtual communities can be 'powerfully "real"' (Danet 1998, p. 131) as can the emotions that accompany them (Danet 1998; Rheingold 1993). This environment would appear to offer useful opportunities for the development of counselor-client relationships. However, there are a number of features of the environment that may complicate the relationship and this may reduce the effectiveness of the counselling process and also raise new ethical issues.

Loss of Identity and Feedback Cues

In Second Life many non-verbal cues are unavailable or limited but it is possible to organize a virtual meeting at a specific location and carry out a dialogue that contains some degree of emotion and has a sense of physical closeness. The avatar may be clothed and customized by the human agent and thus be a recognizable entity. It is within this environment that new forms of counselling may develop. From a counselling perspective Second Life thus surpasses conventional email and chat, however it is certainly still not the same as in real life. The absence of non-verbal cues can still impede the counsellor's ability to assess, diagnose and adequately help the client and consequently increase the risks of breaching the general principle of do no harm.

A counsellor providing a service to an avatar (a client's character) in Second Life, is effectively unaware of the true identity of the individual they are counselling. In a sense this can be regarded as the same position as a client consulting a counsellor with the preamble 'I have a friend who has a problem ...' and is a valid way of approaching counselling. However, one has to ask if it is valid to treat an avatar as an object, a third party, through which counselling can be enacted. In such situations would the advice given, the structure and the content of the counselling session differ if the person was seeking face-to-face counselling? This is a question not easily answered and it is likely the answer would differ depending on the situation. However, counsellors have an ethical responsibility to respect their client, regardless of who they are, while helping them through the counselling process (Geldard & Geldard 2001). To this end it could be argued that, from an ethical perspective, the service delivered to an online avatar should be the same as through face-to-face counselling. This approach, however, relies on a fundamental requirement that the avatar should represent a true facsimile of the human client throughout the counselling process. One problem is that the environment does lend itself to disguise of individuals and the avatar may, or may not, share characteristics with their human counterpart. It is not, for example, unusual for a male to decide to represent themselves as a female when in avatar form (Danet 1998; Asai, 2006). This disguise or role appropriation presents a potential barrier for the counsellor in reaching the 'true' client and places a higher degree of ethical responsibility on the client to be honest in the way that they represent themselves.

If the client does misrepresent themselves to the counsellor the risk arises that advice provided to the avatar which is later enacted by the person behind the avatar could cause harm. This situation is likely to only occur when the avatar persona is so very far removed and different from the real life person. Taylor (1999) researched the effect of online and offline embodiment on online research and proposed that when dealing with bodies in virtual worlds, they be accepted in their own right and not be related back to the offline body behind them. However, Taylor (1999) does highlight that often when communicating to a client they "speak as their avatar, their offline selves or as both" (Taylor 1999,

p.440). During a counselling session counsellors will need to be careful to detect what the real underlying problem is, as opposed to the problem expressed through an intermediary form, and in that way help to avoid the risk of doing harm through incorrectly assessing the situation. It is an interesting issue and one that requires further research.

Second Life does not necessarily provide a platform for counsellors to share the same level of resources or empathic communication with clients as face-to-face counselling. Therefore, while clients may feel better after an online counselling session and not feel the need for further therapy it is unlikely that they will have developed the skills to cope with future situations of high stress and emotions (Childress 2000). Online counselling therefore runs the risk of becoming a 'quick fix' as opposed to a solution and in the long term may be a hindrance to the counselling process. Once again, online counselling in Second Life may indirectly increase the risks of doing harm by leaving the client in a state of dependency rather than in a position of being empowered.

Prentice acknowledges that "the dangers and morality of misrepresentation" (Prentice 2007, p3) are as much a problem within Second Life as they are within any online community. Counselling organisations operating within Second Life will need to be wary of misrepresentation both by the client and themselves. While the client's avatars may not be reflections of their offline selves the counsellor should clearly and consistently present an accurate representation of themselves. It may be acceptable for the client to assume an alternate gender role but the counselor should ensure that they do not similarly misrepresent themselves or ethical issue will emerge.

Confidentiality

Another ethical concern within counselling is confidentiality (Geldard & Geldard 2001; Childress, 2000) and this is particularly at risk with counselling through Second Life. Communications that take place in Second Life "are transmitted across the public Internet and stored (for some period of time, however short) on remote servers" (Prentice 2007, p.3). Further, with the exclusion of private islands and land, all of Second Life is a public forum in which conversations that take place are there for all, within a certain vicinity, to read. Unlike a website environment, the organisation or counsellor currently has very little control over the security within Second Life. There are also possibilities for breaches of confidentiality on the clients end (Childress 2000). Other people who have access to the client's Second Life account can log on and pose as the client and there is no easy way of ensuring that the avatar actually represents the client (Prentice 2007). Likewise, privacy is closely linked to confidentiality. Currently, aside from using an external voice conferencing application, such as Skype, the only way to ensure privacy in Second Life is through the use of a private island (Prentice 2007). Clients would be required to contact the counsellor in Second Life and arrange an appointment time in order to authenticate themselves. At the set appointment time, the counsellor will need to grant the client access to the private island. Confidentiality and privacy in Second Life become shared ethical responsibilities for the client and counsellor alike.

Despite the ethical risks associated with counselling through Second Life, a counsellor has an ethical responsibility to provide help to the client when it is needed (Childress 2000). The ethical risks discussed here are risks that need to be overcome and the counsellor has an ethical responsibility to inform the client of the risks and obtain their consent to continue before engaging in an online counselling session. From an organizational perspective there will also be a need to develop clear policies that can protect the organization in the event that a client knowingly misrepresents themselves and suffers unforeseen consequences as a result of that misrepresentation.

CONCLUSION

The underlying ethics associated with counselling are the same regardless of the method of delivery, be it face to face, electronically mediated or conducted via an avatar. In online counselling environments there are a number of aspects that may raise new areas of risk when compared with more traditional face-to-face counselling. Confidentiality, privacy and security are clearly technical areas of risk that can be improved by including approaches that apply to many other types of online system. Ethical issues arising from deliberate or accidental misrepresentation, pose significantly greater risks where the client may be harmed. It is still early days in the practice of using social networks, such as Second Life, as a platform for the delivery of online counselling but it would appear that these new online environments will require counsellors to develop new models and approaches if they are to provide appropriate and ethical support for their clients. In the future, technical improvements to the Second Life application and other social networks combined with detailed research into counselling in this new environment may lead to new and safe opportunities to reach

and support clients. The literature that is currently available is still rather limited, and the ethical issues surrounding online counselling in Second Life and similar environments are also not well researched. It is clear that there is a place for counselling within the new online social networks and that the extended reach of such services will prove to be valuable in terms of efficiency and efficacy. Utilisation of the more secure facilities offered by such systems as FaceBook will overcome some of the concerns about supporting and delivering an ethical service to clients, but there will still be many challenges facing both individual counselors and the organizations they work for.

REFERENCES

- Asai R. 2006, 'Living with another gender on the Net', *Ethicomp*, viewed June 4 2007, available at <http://www.ccsr.cse.dmu.ac.uk-/conferences/ethicomp/ethicomp2007/abstracts/75.html>
- Belluci, E. & Zeleznikow, J. (2001) 'Family_Winner: A computerized negotiation support system which advises upon Australian Family Law', *Proceedings of the International Society for Decision Support Systems*, 6th International conference, Scoble, R. & Paul, R. J. (eds), Brunel University, London, 2-4 July.
- Chester, A. & Glass, C.A. 2006, 'Online counselling: a descriptive analysis of therapy services on the Internet', *British Journal of Guidance & Counselling*, vol. 34, no. 2, pp. 145-160.
- Childress, C.A. 2000, 'Ethical Issues in Providing Online Psychotherapeutic Interventions', *Journal of Medical Internet Research*, vol. 2, no. 1, viewed 18/08/2007, <<http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1761841>>.
- Christensen, H. & Griffiths, K. 2002, 'The prevention of depression using the Internet', *The Medical Journal of Australia*, vol. 177, pp. 122-125.
- Danet, B. 1998, 'Text as Mask: Gender Play, and Performance on the Internet', in Jones, SG (eds) 1998, *CyberSociety 2.0: Revisiting computer-mediated communication and community*, vol. 2, New Media Cultures, SAGE Publications Inc, USA.
- Egan, G. 1975, *The Skilled Helper: A Model for Systematic Helping and Interpersonal Relating*, Wadsworth Publishing, Belmont California
- Egan, G. 2002, *The skilled helper: a problem-management approach to helping*, 7th Edition, Brooks/Cole Publishing Company, USA.
- Fielden, K. & Goldson, J. (2006) 'ICT-Enabled Communication in the New Zealand Family Court: A Soft Systems Study', *Systems Thinking and Complexity Science: Insights for Action*, Proceedings of the 11th ANZSYS Conference, Christchurch, New Zealand, 5-7 December 2005, Ed. by Richardson, K.A., Gregory, W. J., & Midgley, G., ISCE Publishing, USA.
- Geldard, D. & Geldard, K. 2001, *Basic personal counselling: a training manual for counsellors*, 4th Edition, Pearson Education Australia.
- Mesch, G. & Talmund, I. 2006, 'The Quality of Online and Offline Relationships: The Role of Multiplexity and Duration of Social Relationships', *The Information Society*, vol. 22, pp. 137-148.
- Palaniappan, S. & Jun-E, T. 2006, 'Web-Based Counselling System', in *Fourteenth International Conference of Advanced Computing and Communication*, December 20 – 23, Surathkal, India, p. 50-53.
- Rheingold, H. 1993, *The virtual community: homesteading on the electronic frontier*, HarperPerennial, New York.
- Rochlen, A.B., Zack, J.S. & Speyer, C. 2004, 'Online Therapy: Review of Relevant Definitions, Debates and Current Empirical Support', *Journal of Clinical Psychology*, vol. 60, no. 3, pp. 269-283.
- State of Victoria, Department of Health Services 2002, *New Directions for Victoria's Mental Health Services*, Metropolitan Health and Aged Care Services Division, Melbourne Victoria Australia.
- Taylor, T.L. 1999, 'Life in Virtual Worlds: Plural Existence, Multimodalities, and Other Online Research Challenges', *American Behavioural Scientist*, vol. 43, no. 3, pp. 436-449.

- Williams, D. 2006, 'Virtual Cultivation: Online Worlds, Offline Perceptions', *Journal of Communication*, vol. 56, pp. 69-87.
- Ybarra, M.L. & Eaton, W.W. 2005, 'Internet-Based Mental Health Interventions', *Mental Health Services Research*, vol. 7, no. 2, June, pp. 75-87.
- Asai R. (2006). Living with another gender on the Net, *Ethicomp*, viewed June 4 2007, available at <http://www.ccsr.cse.dmu.ac.uk/-conferences/ethicomp/ethicomp2007/abstracts/75.html>

COPYRIGHT

Rebecca Andary and David A Banks © 2008. The author(s) assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

The Wikipedia: Experts, Expertise and Ethical Challenges

Sharman Lichtenstein

School of Information Systems

Deakin University

Melbourne, Australia

Email: sharman.lichtenstein@deakin.edu.au

Abstract

Participatory models are replacing the traditional models of experts and expertise that are based on individuals, their credentials and domain experience. The Wikipedia is a well-known and popular online encyclopedia, built, edited and administrated by lay citizens rather than traditional experts. It utilises a Web-based participatory model of experts and expertise to enable knowledge contributions and provide administration. While much has been written about the Wikipedia and its merits and pitfalls, there are important ethical challenges stemming from the underlying Wikipedia model. Ethical concerns are likely to be important to Wikipedia users, however as yet, such concerns have not been systematically explored. By reviewing and synthesising existing literature, this paper identifies six key ethical challenges for existing and potential Wikipedia users, stemming from the underlying Web-based participatory model of experts and expertise. Important implications arising from the findings are also discussed.

Keywords

Wikipedia, experts, expertise, knowledge, information ethics.

INTRODUCTION

Understandings of the related concepts - "expert" and "expertise" - are increasingly participatory, rather than individual. Traditionally, an "expert" has been conceptualised as a person who has developed the knowledge, skills (analytical, creative and practical), and abilities with which to succeed in a given domain (Sternberg 2000). Such knowledge, skills and abilities comprise that person's domain-based expertise. By contrast, in the new participatory models of experts and expertise, lay citizens contribute their expertise, sometimes being called "lay experts" by scholars (Kerr et al. 2007; Nowotny et al. 2001).

Importantly, it has been the advent of Web 2.0 and related applications such as *Wikis* and *Weblogs* that has stimulated the development and use of participatory models of experts and expertise. Such technologies provide convenient and ubiquitous global access and an evolving set of innovative tools, enabling lay citizens to contribute their knowledge via a range of relevant participatory models. However, Web-based participatory models of experts and expertise are subject to instrumental manipulation, as are all knowledge management systems (Land et al. 2007). Despite significant development and uptake of various Web-based participatory models of experts and expertise, little is known of the ethical issues involved. By ethical issues in this context we refer to any underlying motives for the introduction of such models, the way the models are used in practice, and the impact of such use on individuals, organisations and society (Land et al. 2007).

In this paper we explore key ethical challenges associated with the use of the *Wikipedia* (Wikipedia.org) as a Web-based participatory model of experts and expertise. The Wikipedia is a well-known collaborative knowledge management system purposed as an online encyclopedia, and characterised by significant lay citizen participation and contribution. The Wikipedia claims to enable ubiquitous access to experts (lay experts) and their expertise.

The rest of the paper is organised as follows. We commence with a brief discussion of traditional notions of experts and expertise, and review several key trends that have motivated new participatory models. We then discuss key concepts underpinning participatory models and review the Wikipedia

approach. As our paper's key contribution, we examine the ethical challenges presented by the Wikipedia in this context. The analysis provided in this paper highlights six important ethical challenges to be considered by current and future Wikipedia users. Finally, we draw conclusions and make final remarks.

TOWARD PARTICIPATORY MODELS OF EXPERTS AND EXPERTISE

As already mentioned, an expert has traditionally been defined as a person who has developed the knowledge, skills (analytical, creative and practical), and abilities to succeed in a particular domain (Sternberg 2000). There are many major and minor variations on this theme to be found in other published theories of experts. For example, according to Weiss and Shanteau, an expert is 1) someone with evaluative skills in his or her domain of specialisation, and 2) someone who can apply such an evaluation to a topic (Weiss & Shanteau 2003). Expertise is defined as the optimal level at which a person is able and/or expected to perform within a specialised realm of human activity (Swanson 1999). Weiss and Shanteau cite various examples of topical expertise including expressing an evaluation as a judgement, projecting from an evaluation to make a prediction, communicating an evaluation to others, and executing an evaluation as a performance (Weiss & Shanteau 2003).

According to traditional perspectives on experts and expertise, expertise is developed in several stages, after which a person is considered an expert. Anderson (1995) identified three steps in the development of expertise – a cognitive stage involving the acquisition of facts, an associate stage involving the application of that knowledge, and an autonomous stage where the knowledge and its application are effortlessly and immediately applied.

The trend toward participatory models of experts and expertise has been triggered by significant changes in public and academic beliefs about knowledge and its method of production. It is increasingly argued that 1) knowledge is a social construct, 2) science policy and scientific knowledge should be situated within contemporary societies, “socially robust” and practically relevant, and 3) scientific development of knowledge should be debated with the marketplace, thus improving knowledge by including lay citizen participation (Frederiksen 2003; Gibbons 1999; Nowotny et al 2001). Further, the public has expressed serious misgivings about traditional experts, including that experts often disagree, make subjective judgements, and are elitists (or represent elitists) (Burchell 2007; Finkelstein 2007; Shanteau 2001).

New models of participatory knowledge production, pluralistic expertise and lay experts have appeared in response to such arguments (Gibbons, 1999). According to Gibbons (1999), expertise emerges from the synthesis of many knowledge sources, with authority linked to the pattern of self-organising connection of those sources. Pluralistic expertise has also been termed “collective intelligence”, crowd-sourcing, or the wisdom of crowds (Surowiecki 2004). The individuals (lay citizens) who contribute to this collective intelligence are the new experts – as mentioned earlier, sometimes termed “lay experts” (Kerr et al. 2007, Nowotny et al. 2001).

THE WIKIPEDIA

Web 2.0 offers useful participatory tools and structures for lay citizens to produce knowledge collaboratively (Fischer 1993). Here we focus on the use of Wikis, which offer conversational collaborative media for knowledge creation (Wagner 2004). A Wiki is “a collaboratively created and iteratively improved set of web pages, together with the software that manages the Web pages” (Wagner 2004, p. 265). It has also been defined functionally as “a freely expandable collection of interlinked web pages, a hypertext system for storing and modifying information - a database, where each page is easily edited by any user with a forms-capable Web browser client” (Leuf & Cunningham 2001, p. 14).

A Wiki has several important advantages for knowledge processes. According to Wagner (2004), a Wiki's main strength is that it supports conversational knowledge creation. Wagner identifies other important benefits of Wikis as their economy, speed, ease of use, and superior value in distributed knowledge environments. A Wiki is also potentially an emancipatory medium as it has a decentralised approach; each receiver is a potential transmitter of knowledge; the masses can be mobilised; knowledge production is collective; participants interact and receive feedback; social control is obtained by self-organisation; and there is a political learning process (Ebersbach & Glaser 2004).

The most well-known example of a Wiki is the Wikipedia, purposed as a popular online open source encyclopedia. An encyclopedia is “a work that contains information on all branches of knowledge or

treats comprehensively a particular branch of knowledge usually in articles arranged alphabetically often by subject” (Merriam-Webster 2007). Online encyclopedias are digital collections of such content. Their advantages over printed encyclopedias include ease of search and retrieval, ease of updating, greater accessibility and leverage of multimedia. These and many other useful functions possible with online encyclopedias are unavailable for traditional printed encyclopedias (c.f. Kolbitsch & Maurer 2005). In this paper we focus on the Wikipedia model of an online encyclopedia and how it utilises lay citizens as experts, developing and leveraging their collective intelligence (supported by published sources) for expertise.

The Wikipedia concept was established in 2001 and has been widely cited as a *successful* online encyclopedia. According to Alexa, a well-known Web traffic information site, the English Wikipedia was the 9th most visited Web site in January 2008. In December 2007 there were more than 2,129,379 million articles in the English Wikipedia (http://en.wikipedia.org/wiki/Wikipedia:Size_comparisons, 16 December 2007) and more than 7 million articles in the collected Wikipedias (Wilkinson & Huberman 2007). Wikipedias exist in a wide range of languages including English, French, Spanish, Italian, Japanese, German and Indonesian. While there has been some recent evidence of decline in article production and activity in 2007 (Rohde 2007), the Wikipedia remains highly popular with seekers of knowledge. However, the popularity of a knowledge source is not a reliable measure of its *knowledge quality*.

Whether Wikipedia-based knowledge – based on lay experts and their expertise – is as *accurate*, *reliable*, and *credible* as users expect of an esteemed online encyclopedic source, is an important *ethical* question. To understand the ethical challenges involved, we must first consider the Wikipedia’s model of knowledge synthesis. The Wikipedia is based on wiki technology and a democratic process where any internet-connected member of the global population may collaboratively create, edit and delete articles, with equal value afforded to each action and contributor. Importantly, articles may be edited by anyone (henceforth termed an editor) and such edits may be challenged by anyone. Indeed, challenged edits frequently revert to earlier versions of articles. Such reversions are decided (after discussion) by volunteer administrators elected mainly on the basis of sufficient numbers of prior Wikipedia contributions, rather than on their topic expertise or contributions’ quality. To date, the Wikipedia has attracted over 10,000 volunteer contributors, most of whom are not domain experts.

A neutral point of view (NPOV) is often cited as the pivotal principle by which edited Wikipedia articles are accepted, reverted or deleted by administrators. A NPOV is the presentation of an article (or part thereof) according to multiple perspectives, rather than only one perspective. Writing with a NPOV is considered important in Wikipedia culture as if an article presents only a single perspective, it might be biased, according to Wikipedia principles.

The Wikipedia can be edited by any person, whose identification and credentials are considered unnecessary. Administrators oversee the Wikipedia process. They are generally not domain experts and are appointed based on substantial cumulative participation rates. Administrators set Wikipedia policies, ban destructive (or perceived-to-be-destructive) users, help resolve disputes, and generally maintain order. They possess significant powers regarding what knowledge is produced and who produces it, although administrator influence on content editing has been reported to be waning (Kittur et al. 2007).

Clearly, users of an esteemed popular online encyclopedia expect its articles to be of a high quality. Some studies have positively associated the quality of Wikipedia articles with 1) the degree of participation - the number of collaborators and amount of collaboration (Anthony et al. 2007; Wilkinson & Huberman 2007), and 2) the incentives provided by personal reputation building (Anthony et al. 2007; Stewart 2005). The Wikipedia links article quality partly to the notion of the “notability” of a topic. Summarising Wikipedia’s notability policy, “a topic is presumed to be notable if it has received significant coverage in reliable secondary sources that are [independent](http://en.wikipedia.org/wiki/Wikipedia:Notability) of the subject” (<http://en.wikipedia.org/wiki/Wikipedia:Notability>). Thus if a topic is not considered notable, it is not considered of sufficient quality to be published. We will say more about this issue in the next section. Several studies have found the English Wikipedia’s articles to be relatively accurate. A recent assessment of a small number of encyclopedia articles found that the English Wikipedia is almost as accurate as the *Encyclopædia Britannica* (Giles 1995). However, the assessment also highlighted the Wikipedia’s confusing and erratic aspects. Such weaknesses have been excused in the past by Wikipedia enthusiasts by pointing out that encyclopedias are only starting points for knowledge

seekers and that links to more specific online knowledge sources are provided in Wikipedia articles for readers who seek more knowledge on a given topic. However many users tend to cite the Wikipedia articles rather than the linked sources. A recent article in BBC Focus magazine reported a comparative study of the accuracy of four online encyclopedias for articles on Avian Flu, Robert Stephenson, and Planetesimal. The study found that the English Wikipedia was marginally more accurate than the other online encyclopedias, including the *Encyclopædia Britannica*. The additional accuracy was attributed to greater currency due to the dynamic nature of the Wikipedia.

ETHICAL CHALLENGES FOR THE WIKIPEDIA

In contrast to the positive reports on the quality of articles in the Wikipedia, discussed above, other reports cite inaccuracies and various unfavourable comparisons. In a recent infamous incident, the Wikipedia published a false article, edited by a prankster, nominating journalist John Seigenthaler Sr. as a suspect in the assassination of Robert Kennedy and President John F. Kennedy. The defamatory article remained in the Wikipedia for four months until Seigenthaler convinced the Wikipedia's founder, Jimmy Wales, to remove it. In a different type of incident, Thomas Vander Wal, who developed the term "folksonomy", experienced considerable difficulty having his definition accepted for the Wikipedia. Clearly, there are concerns with the Wikipedia which may lead users to doubt the veracity of the expertise provided, and the credibility of the experts who contribute its content.

We now discuss six important ethical concerns with the Wikipedia. *First*, the very people interested and experienced (while possibly uncredentialed) in a given domain, who are potentially able to source an article's notability (by finding an independent source), do not regularly visit Wikipedia in order to contribute to the discussions on the notability or validity of that topic. Thus specialised articles can be too easily deleted as "unnotable". Administrators, who are not selected because they have domain expertise, subjectively decide whether an article is notable, based on their interpretation of Wikipedia's definition of notability. The omission of non-notable articles is contrary to the participatory inclusive approach intended for the Wikipedia. However, such omissions are essential to an encyclopedia which should not be a compendium of *all* knowledge, no matter how trivial. Thus the collection of articles in the Wikipedia has not been selected according to prior organisation of the most important knowledge for inclusion. Rather, the knowledge made available is present due to different interpretations of relevance by administrators, who themselves are not domain experts and who lack the experience to make such judgements.

Second, and following from the first concern expressed above, the method of selection of topics for inclusion by editors – that of notability – is a form of discrimination (elitism) (Noah 2007). However, a need to avoid elitism was a key influence motivating the shift from traditional individual models of experts and expertise to participatory democratic models. It appears that the Wikipedia does not democratise knowledge by an inclusive approach, but rather provides a new oligarchy, based on administrator beliefs regarding topic relevance.

A *third* criticism of the Wikipedia's content quality arises from the anonymity of many editors and administrators. Prior to December 2005, Wikipedia allowed anonymous postings, which encouraged vandalism and reduced the quality of some articles. After several well publicised incidents, it was decided to disallow new articles by anonymous contributions. However in 9 November 2007, the ability to create anonymous articles was reinstated for a trial period due to a significant decline in the growth of the number of articles in the Wikipedia (Wikinomics 2007). At the time of writing, the results of this reinstatement are unknown. It should be noted, however, that it is the one-time contributions of anonymous contributors which *may* provide the highest quality contributions (Anthony et al. 2007). It is not known whether such contributors are experts in the traditional sense (that is, by virtue of credentials and experience). In either case, with anonymity comes a lack of accountability, and inaccurate, potentially harmful knowledge creeps into the Wikipedia as the writers cannot be traced. The reliance on others to detect, report and correct inaccurate and harmful knowledge is a risky strategy. Finally, and importantly, with anonymity one does not know who wrote an article and a reader cannot evaluate an article based on the credibility of the source as the source's identity is unknown.

Fourth, the Wikipedia favours a few "new-elite" users. A small group of elite users (with 10,000 or more edits) is dominating edits, although the proportion of total edits that the elite users perform has fallen from around 50% in 2002 to 20% in mid-2006 due to increased involvement by users with fewer

than 100 edits (Kittur et al. 2007). Thus the Wikipedia is, in fact, constructed by a few powerful people, rather than the democratic participation of the masses as originally intended.

Fifth, there is significant role switching between administrators and editors leading to the loss of many content creators (that is, editors) (Anthony 2007). As there is power in the administrative role, and many well-meaning editors are treated poorly by administrators, there is a tendency for editors to abandon content creation for an administrative role, once they become significantly involved.

Sixth, the Wikipedia places too much power in the hands of administrators, who have recently been accused of covert collaboration via an administration mailing list, where individual editors are targeted for banning based on assumed “sock-puppetry” (Metz 2007). When a new editor edits an article for the first time and appears (to administrators) to know too much about the intricacies and nuances of Wikipedia article-editing, administrators often identify that person as a “sock puppet” and revert the article to its prior content. However mistakes are made in such sock-puppet identification, and it is clear that many genuine editors are unable to edit articles without risking being mistaken for a sock puppet, or otherwise mistrusted. The political practices of the administrators at this time are not adequately monitored and the risks of mistreatment and unfairness rise accordingly.

CONCLUSION

We have shown in this paper how the Wikipedia adopts a Web-based participatory model of experts and expertise. The paper highlights six key ethical issues for potential and current Wikipedia users to consider. Several scholars have noted that users seek greater assistance in assessing the expertise present in the Wikipedia and similar online encyclopedias. Knowledge seekers must have a way to determine whether they can trust a claimed expert and his or her expertise (Goldman 2002) and possessing “meta-expertise” may be helpful. “Meta-expertise” is the ability to assess expert credibility by judging demeanour, internal consistency of expert remarks, appropriateness of social locations and so on (Collins & Evans 2007). Ratings of experts by meta-experts can be useful cues to the credibility of such experts. While such cues are currently unavailable in the Wikipedia, emerging approaches have potential. For example, Adler and Alfaro (2007) have developed a reputation system for the Wikipedia based on whether edited words persist over time. The assumption is that if others do not change the words, then the words have value, and their author (that is, the editor who wrote those words) can be trusted in future to provide valuable content. Priedhorsky et al (2007) measure the value and thus reputation of an article’s editor based on the number of times the editor’s words have been viewed. While these initial attempts at helping users to better estimate the value of a Wikipedia article are important steps, they go only a small way toward addressing the six ethical challenges highlighted in this paper. If the Wikipedia model is to survive and thrive, the ethical issues must be fully illuminated and better addressed, requiring further research and the development of effective solutions.

REFERENCES

- Adler, B.T. and de Alfaro, L. 2007, ‘A content-driven reputation system for the Wikipedia’, *Proceedings of the 16th International Conference on World Wide Web*, Banff, Alberta, Canada, pp. 261-270.
- Anderson, J.R. 1995, *Cognitive Psychology and its Implications*, 4th edn, New York: W.H. Freeman and Company.
- Anthony, D., Smith, S.W. and Williamson, T. 2007, *The Quality of Open Source Production: Zealots and Good Samaritans in the Case of Wikipedia*, Dept of Computer Science, Dartmouth, Technical Report TR2007-606.
- Anthony, S. 2007, ‘Where have all the writers gone: The diversion, distraction and departure of wiki “Content Creators”’, *Proceedings of Wikimania 2007*, Taipei.
- Burchell, K. 2007, ‘Empiricist selves and contingent ‘others’: the performative function of the discourse of scientists working in conditions of controversy’, *Public Understanding of Science*, vol. 16, no. 2, pp. 145-162.
- Collins, H. and Evans, R. 2007, *Rethinking Expertise*, The University of Chicago Press.
- Ebersbach, A. and Glaser, M. 2004, Toward Emancipatory Use of a Medium: The Wiki, *International Journal of Information Ethics*, vol. 2, pp. 1-9.

- Finkelstein, S. 2007, Post in 'Knowledge Access as a Public Good', Danah Boyd, 27 June, *Encyclopedia Britannica Blog*, url: <http://blogs.britannica.com/blog/main/2007/06/knowledge-access-as-a-public-good/> (accessed 21 January 2008)
- Fischer, F. 1993, Citizen Participation and the Democratization of Policy Expertise: From Theoretical Inquiry to Practical Cases, *Policy Sciences*, vol. 26, no. 3, pp. 165-187.
- Frederiksen, F., Hansson, F. and Wenneberg, S. 2003, 'The Agora and the Role of Research Evaluation, Evaluation', *Evaluation*, vol. 9, no. 2, pp. 149-172.
- Gibbons, M. 1999, 'Science's New Social Contract with Society', *Nature*, vol. 402, pp. 11-18.
- Giles, J. 1995, 'Internet Encyclopaedias go Head to Head', *Nature*, vol. 438, pp. 900-901.
- Goldman, A.I. 2002, *Experts: which ones should you trust? Pathways to knowledge*, pp. 139-164, Oxford Scholarship Online Monographs.
- Kerr, A., Cunningham-Burley and Tutton, R. 2007, 'Shifting Subject Positions: Experts and Lay People in Public Dialogue', *Social Studies of Science*, vol. 37, no. 3, pp. 385-411.
- Kolbitsch, J. and Maurer, H. 2005, 'Community building around encyclopaedic knowledge', *Journal of Computing and Information Technology*, vol. 14, no. 3, pp. 175-190.
- Kittur, A., [Chi, E. H.](#), [Pendleton, B. A.](#), [Suh, B.](#) and Mytkowicz, T. 2007, Power of the few vs. wisdom of the crowd: Wikipedia and the rise of the bourgeoisie, *Proceedings of 25th Annual ACM Conference on Human Factors in Computing Systems (CHI 2007)*, April 28 - May 3; San Jose; CA.
- Land, F., Nolas, S-M., and Amjad, U. 2007, 'The Ethics of Knowledge Management', *International Journal of Knowledge Management*, vol. 3, no. 1, pp. 1-9.
- Leuf, B. and Cunningham, W. 2001, *The Wiki Way: Collaboration and Sharing on the Internet*, Reading, MA: Addison-Wesley.
- Merriam-Webster 2007, Merriam-Webster Dictionary, url: <http://www.m-w.com/> (accessed 21 January 2008).
- Metz, C. 2007, 'Secret Mailing List Rocks Wikipedia', *The Register*, UK, 4 December, url: http://www.theregister.co.uk/2007/12/04/wikipedia_secret_mailing/ (accessed 21 January 2008).
- Noah, T. 2007, 'More on Wikability', *Slate*, March 1, url: <http://www.slate.com/id/2160839/> (accessed 21 January 2008)
- Nowotny, H., Gibbon, M. and Scott, P. 2001, *Re-thinking science. Knowledge and the public in an age of uncertainty*, Oxford: Polity Press.
- Priedhorsky, R., Chen, J., Lam, S-K., Panciera, K., Terveen, L. and Riedl, J. 2007, Creating, Destroying, and Restoring Value in Wikipedia, *Proceedings of GROUP'07*, Sanibel Island, Florida, url: <http://www-users.cs.umn.edu/~reid/papers/group282-priedhorsky.pdf> (accessed 21 January 2008)
- Rohde, R. 2007, The Statistical Decline of the English Wikipedia Community, url: <http://lists.wikimedia.org/pipermail/wikien-l/2007-October/082562.html> (accessed 21 January 2008)
- Shanteau, J. 2001, What Does it Mean When Experts Disagree? In G. Klein & E. Salas (eds.), *Naturalistic Decision Making*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Sternberg, R.J. 2000, 'What is Practical Intelligence?' in Sternberg, R.J., Forsythe, G.B., Hedlund, J., Horvath, J.A., and Wagner, R.K. (eds.) *Practical Intelligence in Everyday Life*, Booktopia, pp. 1-10.
- Stewart, D. 2005, 'Social Status in an Open Source Community', *American Sociological Review*, vol. 70, pp. 823-842.
- Surowiecki, J. 2004, *The Wisdom of Crowds: Why the Many are Smarter than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*, Doubleday.
- Swanson, R.A. 1999, 'The foundations of performance improvement and implications for practice', In R. Torrance (ed.), *Performance Improvement Theory and Practice*, pp. 1-25, San Francisco, Berrett-Koehler.

- Wagner, C. 2004, Wiki: A Technology for Conversational Knowledge Management and Group Collaboration, *Communications of AIS*, vol. 13, no. 9, pp. 265-289.
- Weiss, D.J. and Shanteau, J. 2003, 'Empirical Assessment of Expertise', *Human Factors*, vol. 45, pp. 104-114.
- Wikinomics 2007, 'Is Wikipedia Peaking?' Blog, url: <http://www.wikinomics.com/blog/index.php/2007/06/14/is-wikipedia-peaking/> (accessed 21 January 2008)
- Wilkinson, D. and Huberman, B. 2007, 'Cooperation and Quality in Wikipedia', *Proceedings of WikiSym'07*, October 21-23, Montreal, Canada, url: <http://www.hpl.hp.com/research/idl/papers/wikipedia/wikipedia07.pdf> (accessed 21 January 2008)

COPYRIGHT

Sharman Lichtenstein ©2008. The author assigns to Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The author also grants a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the author.

Security and Ethical Issues in the Virtual World of Second Life

Chia Yao Lee

School of Information Systems
Deakin University, Australia
chia.lee@deakin.edu.au

Abstract

In recent times, Virtual Worlds such as Second Life have generated substantial publicity due to the participation of Fortune 500 companies, and other public and private organisations. As practitioners continue to discuss how organisations could derive business value from Virtual Worlds, new security and ethical issues in Virtual Worlds have emerged to challenge Virtual World users and stakeholders. This paper discusses privacy, intellectual property and a host of other security and ethical issues in Virtual Worlds. It contributes to practice and research by (i) providing insight into emerging security and ethical issues in Virtual Worlds, (ii) analysing the implication of these issues, within and beyond Virtual Worlds, and (iii) raising awareness on security and ethics among Virtual World users and stakeholders.

Keywords: Virtual World, Security, Ethics, Intellectual Property, Privacy

INTRODUCTION

When Business Week first published its cover story on Virtual World entrepreneur Anshe Chung in May 2006 (Business Week 2006a), it quickly projected the Virtual World of Second Life into the boardrooms of Fortune 500 companies. In 2006 and 2007, Virtual Worlds, in particular Linden Lab's Second Life, have received substantial press coverage due to the participation of several well known public and private organisations. IBM, a pioneer in Virtual World research and adoption, has plans to spend US\$100 million in Virtual World related projects (Business Week 2006b). After initial success with Webkinz and Club Penguin, the Walt Disney Company is currently developing ten new Virtual Worlds, at a cost of US\$5-10 million apiece (Barnes 2007). These actions point to the high level of interest shown by the corporate world in Virtual Worlds and the potential that they recognise in these ventures.

Virtual Worlds have also gained notoriety in recent times due to emerging issues in security and ethics. As more aspects of modern society are mimicked, mirrored and extended into Virtual Worlds, and socio-economic activities in Virtual Worlds increase in sophistication, there is little doubt that the scale, depth and number of security breaches and ethical conflicts in Virtual Worlds will also escalate. The collapse of Ginko Financial, a virtual bank in Second Life, has led to practitioners, regulators, consumer advocates and individual users arguing for greater regulation, governance, accountability and transparency in the Virtual World economy. Economists have even compared Ginko Financial's operation to that of a Ponzi scheme (Hutcheon 2007; Reuters 2006). Linden Lab has subsequently moved to ban interest-bearing banking operations in Second Life by individuals and organisations that do not hold a valid banking license in the real world (Reuters 2008a). This move takes effect from 22 January 2008. The CopyBot and Grey Goo attacks in Second Life (BBC News 2006; Lemos 2006) highlight issues with Virtual World security. The CopyBot application enables unauthorised copies of virtual products to be made, raising concerns on the issue of intellectual property piracy and infringement in Virtual Worlds. The Grey Goo attack involves self-replicating virtual objects that mushroom at various locations in Second Life. The Grey Goo attack illustrates the vulnerability of Virtual Worlds to worm attacks, and provides insight into how a Denial of Service attack may disrupt the Virtual Worlds.

In the face of these negative publicity, community and business interest in Virtual Worlds are not expected to diminish altogether. Much like how E-Business had survived the Dotcom Bubble of 2000, Virtual Worlds are expected to survive the initial hype and negative publicity. Garter Consulting predicts that by 2011, close to 80% of all active Internet users and Fortune 500 companies will engage Virtual Worlds, although not necessarily only in Linden Lab's Second Life (Business Wire 2007). Forrester forecasts that Virtual Worlds are on the brink of becoming a valuable work tool (Forrester

2008). A better comprehension of Virtual World security and ethical issues is instrumental in the effort of making Virtual Worlds a legitimate platform for commerce, education, politics and other socio-economic activities.

As part of a more comprehensive study into Virtual Worlds, this paper analyses a series of security and ethical issues in Virtual Worlds – privacy, intellectual property, freedom of expression, and safety of users and stakeholders. The Virtual World of Second Life has been chosen over other Virtual Worlds due to the wide scope of socio-economic activities and events that take place within it; as well as the large number of real life businesses which have participated in Second Life. However, due to the dynamic nature of activities and events in Second Life, the range of security and ethical issues discussed in the paper is by no means exhaustive.

The paper is organised as follows. providing a brief discussion of Virtual Worlds, presenting an overview of activities and events that take place in Second Life as a basis for discussing security and ethics in Second Life. A discussion regarding Virtual World security and ethical issues in detail. It analyses the implication of these issues, activities and events within, as well as beyond the boundaries of Second Life. Finally the summary of paper, highlighting contributions of the paper, and suggesting future research directions.

What are Virtual Worlds?

Virtual Worlds are computer-generated 3D environments that enable users to interact with one another, as well as with other entities in the environment. Users establish an avatar, which is an online digital representation of the user. The avatar is usually shaped like a human although many Virtual Worlds allow avatars to take the form of other living and non-living things. Virtual Worlds are also known as Synthetic Worlds (Castronova 2005) since elements of the “world” are created artificially. Virtual Worlds such as Linden Lab's Second Life, Makena Technologies' There, and ActiveWorlds Inc's ActiveWorld are commonly referred to as a Multi-User Virtual Environment (MUVE) (Robins 2007) as they enable users to interact with one another in an alternative reality that does not exist physically. NASA uses the term Immersive Synthetic Environment (Laughlin 2007) to encapsulate the idea that Virtual Worlds enables users to experience an immersive virtual reality environment. Many Virtual Worlds support Real Money Trading (RMT), whereby users may convert the Virtual World currency into real world currencies.

Often, Virtual Worlds are incorrectly categorised as video games of the Massively Multiplayer Online Role Playing Game (MMORPG) variety. The fact that many MMORPGs utilise a computer-generated 3D gaming environment does not make all Virtual Worlds an MMORPG by default. In MMORPGs, game players are challenged to achieve game objectives in accordance with game regulations, whilst occupying a specific role or position, such as a soldier, a leader or a monster. Systems exist within MMORPGs to reward or punish players according to the achievement of game objectives, and/or adherence to game regulations. Virtual Worlds differ by not having explicit specific game objectives, game rules and role-play.

Second Life

As previously mentioned, Second Life is a Virtual World founded by Linden Lab. Many elements within Second Life are co-developed, operated and owned by its users. The Second Life Virtual World is known as the “Grid”, and users are referred to as “residents”. The “Second Life viewer” is a client-side application used for accessing 3D content on the Second Life Grid. The viewer is analogous to a 3D web browser. As of January 2008, there are 12 million residents in Second Life, of whom 914,305 have logged in to the Grid in the past 30 days (Second Life 2008a). At any one time, anywhere between 30,000 to 50,000 residents are “inworld”, ie. logged on to the Second Life Grid. Latest statistics show that the majority of residents fall in the 25-34 age group, with the USA, Germany and Japan accounting for residents who spent the longest hours inworld (Second Life 2008b). Second Life's virtual economy is underpinned by the Linden Dollar (L\$). This virtual currency is convertible to real world currencies such as the US Dollar at online exchanges, at the rate of L\$270 to US\$1. On an average day, more than US\$1 million worth of economic activities take place on the Grid.

Apart from obtaining an avatar to establish a presence in Virtual Worlds, individuals and organisations may also choose to operate a piece of virtual land. They can purchase or lease a plot of virtual land, which will give them control over various aspects of the land and activities that take place on the land.

Land owners incur a monthly tier fee for the privilege of owning land. Graphics for items and avatar activities on the virtual land are hosted by Linden Lab computer servers. As such, Second Life land owners are in effect paying Linden Lab for computing resources and bandwidth usage.

Activities and Events in Second Life

To better understand some of the security and ethical issues that may exist in Second Life, this section provides an overview of activities and events in Second Life. The fact that many Virtual World activities and events are in fact a replica, simulation or extension of their real world counterparts ensures that Virtual World activities and events are as sophisticated as real world activities and events, if not even more so.

Virtual World activities and events in Second Life could be categorised into four broad categories:

(i) Business and Commerce

Real world businesses have used Second Life to support a plethora of activities, ranging from marketing and customer support, to product development and retailing (Hemp 2006). The collaborative nature of Virtual Worlds enables businesses to conduct focussed group discussions, obtain customer input for future products, and experiment with innovative retail concepts. For instance, Vodafone has developed the InsideOut product that enables Second Life residents to make and receive voice calls and text messages on their real world mobile phones to/from other Second Life residents (Vodafone 2008). Cisco and IBM utilise Second Life to host business meetings and conferences for their employees, customers and suppliers (LaPlante 2007; Wagner 2007). Second Life has also become a popular platform for product launches. Mercedes Benz launched its 2007 C-Class sedan in Second Life a few days after the real life model was launched (Automotive Portal 2007). Second Life residents were able to test drive this virtual C-Class vehicle on a driving track on Mercedes Benz's Second Life island.

Virtual World businesses (such as Anshe Chung Studios, a Second Life-originated businesses) have also mushroomed to provide a range of virtual goods and services to their avatar customers. Some have gone into avatar fashion and apparels, virtual homeware, and virtual land development. Reverse product placement opportunities exist for Virtual World businesses to introduce new products into the real world, based on products that originated from Virtual Worlds (Edery 2006). One example of this is the Tringo computer game. It was originally developed in Second Life for its residents (Thompson 2006). Versions of Tringo were subsequently released in the real world for PCs and Gameboy Advance.

(ii) Media, Entertainment and Arts

Media, entertainment and arts represent another category of activities in Second Life which is gaining popularity. Reuters and SkyNews have established inworld newsrooms, to report on Second Life activities and events, as well as for presenting real world news content to Second Life residents. Media companies have used Second Life to stream video and audio content, and for hosting live or recorded events for their audiences. For two years in a row now, Reuters has conducted live interviews with attendees of the World Economic Forum at Davos, Switzerland, on its Second Life island (Reuters 2008b, WEF 2007).

Musical performers have held virtual concerts in Second Life by streaming live or pre-recorded work to various Second Life locations. Visual artists have also used Second Life to exhibit their artwork, ranging from 3D sculptures and visual arts to real world and Virtual World photography. Machinimas – animated films created in Virtual Worlds, starring avatars, have also gained popularity. HBO has recently purchased the North American television rights to a machinima filmed entirely in Second Life (Reuters 2007a).

(iii) Education, Training and Research

Over a hundred universities and education institutions have set up virtual campuses in Second Life. Harvard University has conducted courses that require students to attend regular classes inworld since 2006. Other universities have used Second Life to support classroom activities, long distance learning, collaborative group learning, and for distributing course material (Timson 2008). Thompson's NetG learning centre in Second Life is used to conduct technical training courses for its corporate clients, whereas the US military uses the Defense Advanced Research Projects Agency's (DARPA) simulations to train soldiers (Chatham 2007).

In research, there are opportunities for using Virtual Worlds in medical research. For instance Lofgren and Fefferman (2007) discuss how interactions between avatars can be used to model real world epidemics and pandemics. The Idaho State University's Second Life campus has been used for

disaster response training (Stott 2007). Opportunities also exist for socio-economic and computer science studies (Bainbridge 2007), to exploration of interaction between humans and computers, as well as between humans.

(iv) Politics and Government Services

During the 2007 French presidential election, all four presidential candidates extended their election campaigns inworld. The Second Life platform enabled the presidential candidates to engage voters, and interact directly with the so-called community grassroots. The Second Life campaign by Jean-Marie Le Pen was marred by grieving attacks when protesters and Le Pen's security forces engaged in a virtual war (Moore 2007).

A replica of the US Capitol Hill was created in Second Life in January 2007 to coincide with the opening of the 110th US Congress (Reuters 2007b). Attendees of the events were invited to pose questions to Representative George Miller of the Democratic Party. Presidential candidates in the forthcoming US elections have also extended their campaigns inworld, with supporters for Hillary Clinton and Barack Obama having established Second Life campaign headquarters for their candidates.

Apart from political campaigns, government agencies have also used Virtual Worlds to promote tourism and offer government services. The Mexican Tourism Board recreated the Chichen-Itza archeological site in Second Life to promote tourism (Clark 2007), whereas the Swedish government established a Second Life embassy to provide insight into Swedish culture and background (Simmons 2007).

Security and Ethical Issues in the Virtual World of Second Life

This section investigates two important security and ethical issues in the Virtual World of Second Life – Privacy and Intellectual Property.

Privacy and Virtual Worlds

Privacy in the context of Virtual Worlds can be viewed from two distinct perspectives. The first relates to the privacy of Virtual World users in real life, i.e. protection of user/stakeholder identities and contact details in real life. The second relates to the protection of avatar privacy, as in interactions between avatars, activities and events that avatars attend, and land and other virtual properties that avatars own. The second perspective may also relate to issues such as how to prevent visiting avatars from video-capturing an event or sending unsolicited chat messages to other avatars of a group.

These two major privacy perspectives above can be used as guidance when discussing the two privacy issues below, namely (i) Bots and (ii) Griefing, Stalking and Bullying.

(i) Bots in Second Life

Bots are automated avatars, scripted objects that have been programmed to perform certain tasks independent of direct continuous human input. Individuals and organisations in Second Life may program bots to function as greeters to welcome visiting avatars, in the form of kiosks that give out instructions or freebies. Bots have also been designed for training and coaching purposes, and to function as part of security systems to keep intruders out.

Privacy-related controversies have emerged due to the manner with which bots have been used to collect information about virtual land, virtual property, avatars and avatar activities, without the consent of the land/property owners or avatars being observed. Data scraper-type bots such as Electric Sheep Company's "Grid Shepard" have been designed to roam the Second Life Grid to seek out information regarding virtual items which are available for sale, and to catalogue these items and their location on a central database to facilitate more efficient searches (Second Life Herald 2007). Potential buyers could then locate an item and "teleport" (i.e. virtual hyperlink) directly to the virtual location to purchase the item. However, residents who have made their virtual land publicly accessible may have invited probing visits by the Grid Shepard unwittingly. Virtual items which are not meant for sale could be snapped up by other buyers if the owner or creator has not changed the item's "for sale" setting to "not for sale". Potentially, land owners find their islands swarmed by visitors due to the attraction of misleading or outdated sale information listed by bots. Such visits may slow down the performance of

the computer server hosting the virtual island, and turn away genuine customers and visitors when the island's graphic rendering performance is degraded.

Another type of bot in Second Life is known as Landbots (Reuters 2007c). Landbots roam the Second Life Grid to seek out land parcels which are available for sale. Some of the Landbots have been scripted to purchase land parcels on behalf of bot owners if the land parcels are listed at below market price. Landbot owners may have an unfair advantage over other residents, and their operations may be deemed anti-competitive because landbot operations may influence the market for virtual land. Genuinely low priced land becomes inaccessible to newbie residents who cannot compete with Landbots. There have been reports of Landbots disrupting private land transactions between residents, leading to a potential legal action in the real world (Reuters 2007c).

The emergence of bots in Second Life has raised several privacy concerns. Firstly, owners of the bots frequently adopt an Opt-Out participation scheme rather than an Opt-In scheme (Second Life Herald 2007). To protect private property from bots, it has become the responsibility of property owners to secure their land and virtual possessions, by either making their land parcels inaccessible to the public totally, or not displaying their virtual items on the land. In extreme cases, it is analogous to an owner of a virtual item to find his possessions advertised for sale in the classifieds even without placing an advertisement. He would have simply forgotten to remove the item's price tag after the original purchase of the item. Furthermore, it is often too late for owners to reverse a transaction when the problem is detected.

Secondly, information regarding the roll-out of bots has been less than forthcoming. Owners of the bots do not actively publicise the introduction of their bots, nor the policies governing the use of those bots. As such, residents may have little knowledge regarding the existence of such bots, or how the bots probe their possessions and their virtual land parcels. Although Second Life's Terms of Service have explicitly prohibited the introduction of viruses, trojan horses, worms, spywares and other malicious wares, there is a blurry line in defining what bots are – whether the bots are prohibited, which bot activities are contravening the Terms of Service and which are not. Another problem relates to real world jurisdiction that governs the legality of bots. Furthermore, questions arise as to which party would be charged for any misuse of computing capacity and bandwidth due to the emergence of bots – should the bot owners compensate the land owners? Or should land owners accept this responsibility as their products could be found more easily by potential customers?

Thirdly, comparisons have been made between bots in Virtual Worlds and web crawler applications in the traditional 2D Internet (Second Life Herald 2007). Whilst search companies may use web crawler applications to collect static information from 2D websites on the Internet, Virtual World bots may collect an even broader scope of information, including avatar activities and events. Data scraper bots in Virtual Worlds may roam about, collecting information about virtual properties, about avatars, about activities and events that take place on a virtual land, about participants of activities and events, and about the behaviour of the participants, all without the consent or knowledge of users.

Fourthly, such bots may be programmed to operate stealthily. If the presence and existence of bots are not publicised or easily detected, then it is possible for bots to be programmed to perform illegal wire-tapping-like activities. In the real world, business owners strictly forbid their competitors from sending in agents to check on the pricing of products, inventory or product variety; but the existence of bots in Virtual Worlds may allow such activities by competitors, without the knowledge of business owners. Are bots that operate without the knowledge of land owners comparable to intruders that are trespassing?

Fifthly, bots may be programmed to function as trojan horses, keystroke loggers, worms, spywares and malwares that leave a trail of destruction, if not just a disruptive one. Such bots may produce Denial of Service attacks, or create spam-like effects if they generate unsolicited visits and uninvited guests to a virtual land. Thus, the question becomes, are bots comparable to malwares that scan users' computers which are already deemed illegal in many countries?

Last but not least, whilst it may be possible for bots to be programmed to perform anti-intrusion activities to keep out other bots or uninvited visitors, for the anti-intrusion systems to work effectively, these functions may infringe on the privacy of innocent visiting avatars. In the real world, debates are rife with regards to the introduction of CCTV security cameras with automated facial and pattern-recognition systems that monitor crowds to detect unlawful persons or activities. A similar issue may arise in Virtual Worlds, whereby the privacy and freedom of innocent Virtual World users (Balkin 2004)

may be traded off to increase the safety and security of an individual avatar (e.g. the owner of a property).

(ii) Griefing, Stalking, and Bullying

The issue of stalking, bullying and assault in Virtual Worlds is often labelled as griefing attacks. As many Second Life residents perform a broad range of activities in the Virtual World that replicate their real world activities, e.g. socialising and networking, it may be possible for their behaviour to be monitored by other residents, resulting in griefing, stalking, bullying and other anti-social attacks. On traditional 2D Internet, perpetrators have been known to use chatrooms, instant messengers, online forums, blogs and even auction websites to harass, defame, stalk and bully their victims.

Residents of Virtual Worlds may be exposed to even greater risks of harassment and griefing attacks since the Virtual World activities that they participate in are more immersive by nature. Also, there is a host of rich multimedia channels available for propagating such the griefing attacks. The lack of policing and monitoring by independent parties in Virtual Worlds has further worsened the problem. Computing forensics in Virtual Worlds is a challenge if ever a legal case is to be put forward in the real world, due to the difficulty in accumulating evidence, or confirming the veracity of events in Virtual Worlds.

It is also possible for organisations to be victims of griefing attacks. For example, an unclothed, streaking avatar may attend and disrupt formal business events. The Second Life interview of Anshe Chung in December 2006 was disrupted when griefer used large, obscene virtual items to flood the Second Life island where the interview was being conducted (Terdiman 2006). The Virtual World of Second Life is rife with scripted push-guns that displace avatars, and cage weapons that restrict the movements of avatars. Whilst such weapons are a mere annoyance to experienced residents, they have a more profound effect on newbie users, as confirmed by a study by University of Nottingham researchers (University of Nottingham 2007).

Another issue that is related to griefing in Virtual Worlds relates to user-authentication in Second Life. Although when creating a Second Life avatar account, residents are required to include real life personal information, it is still possible for users to create alternative avatars, or alts, that are not authenticated. Thus, there is little that can be done if a griefer uses multiple avatars to stalk and bully his victims. A major problem may arise when griefing is extended into the real world once the real world identity of the victim is hacked into, or when observations of the victim's behaviour in Virtual Worlds lead to identification of the victim, or possible identity theft. Similarly, if the perpetrator and victim have known each other in real life, there is a possibility for real world bullying and stalking to extend to Virtual Worlds.

Griefing in Virtual Worlds have also been used to blackmail and extort residents (Lazarus 2006). Land Griefing is a technique used to affect the sale price land parcels. Sometimes, ugly, high visual impact advertising banners are placed at strategic locations on a virtual island, affecting the land value of neighbouring land parcels, making them less desirable to potential buyers. Land and other types of griefing could be used in blackmails and extortions, especially when the victim does not possess sufficient knowledge or resources to overcome the griefing attacks. There have been examples where Virtual World activities and events have led to real world assault and criminal activities (Sydney Morning Herald 2005). Disruptive, disparaging and inflammatory behaviour by avatars that intervenes financial transactions or disrupts the smooth operation of a virtual event may also be labelled as griefing attacks. The Grey Goo attack (Lemos 2006) has demonstrated how a malicious griefing attack may lead to Denial of Service effects.

For Second Life users and stakeholders, apart of equipping themselves with technical know-how on how to address privacy threats in the Virtual World, there is not much that can be done other than reporting the privacy breaches to Linden Lab. Thus if privacy awareness is heightened amongst users and stakeholders, and they are made to understand the nature griefing; it may be possible for simplistic and low level privacy threats to be diminished.

Intellectual Property

The issue of intellectual property protection in Virtual Worlds faces several new challenges in Virtual Worlds. Although some are simple variations to intellectual property issues in the traditional 2D Internet new methods for piracy, plagiarism and unauthorised duplication have arisen. Legally, intellectual property issues in Virtual Worlds are challenging existing legislative frameworks, often due to a lack of precedence, as well as a lack of suitable legislative acts to address specific types of intellectual property infringement.

The intellectual property issue in Virtual Worlds could also be viewed from two perspectives. The first relates to the protection of intellectual property for Virtual World creations, such as avatar clothing, virtual homeware, virtual land design and architecture, and the scripts that are used to animate virtual items. The second relates to the protection of intellectual property of items in the real world, for example, the creation of a virtual BMW vehicle in Second Life by an unlicensed third party, or the use of trademarked materials. Due to the heavy reliance of the virtual economy on the trading of virtual items and services, piracy and intellectual property infringement of both types may threaten the viability of Virtual World economy.

(i) CopyBot and Unauthorised Use and Virtual World Intellectual Property

The emergence of the CopyBot application in late 2006 (BBC 2006) has raised concern among Second Life residents due to the ease for their virtual possession to be duplicated. The CopyBot application was adapted from a program which was originally used for debugging purposes. The duplication of virtual items in Second Life is not a major technical challenge, as there is a lack of encryption in the transfer protocol between Second Life computer servers and the user's Second Life viewer application. Data transfer between the server and client could be easily monitored and duplicated by third parties.

Apart from the CopyBot issue, virtual items in Second Life could be duplicated as each virtual creation could be analysed at high granularity. It is not impossible for a virtual item to be reversed engineered. Furthermore, unauthorised duplicates would be difficult to determine, due to a lack of authentication and verification methods in Second Life in confirming the identity of the original creator, or of the current owner of a virtual item. Loopholes to crash Second Life servers to initiate a rollback process is well known to hackers as a simplistic approach to making unauthorised duplicates of virtual items in Second Life. A possible method to overcome low level piracy and simple duplication is to include activation passwords to virtual items. The ease of piracy, or the lack of mechanism to combat piracy in Virtual Worlds are by no means a reasonable excuse for piracy of virtual goods. The copyright infringement lawsuit by Kevin Alderman against avatar Volkov Catteneo represents a well known example whereby piracy of virtual items had been brought to a real world court for settlement (Reuters 2007d).

(ii) Unauthorised Use of Real World Intellectual Property

The other intellectual property related issue is quite different from CopyBots and unauthorised reproduction of virtual items. It relates to the unauthorised use of copyright protected items, intellectual property and trademark in Virtual Worlds. The unauthorised reproduction of real item, albeit virtually, infringes existing copyright legislation, but such cases are still difficult to prosecute in a real world court as minute details of a virtual item could be altered and thus introduce marked differences between the virtual item and its real world counterpart. In the case of unauthorised use of trademarked materials, it may be easier for trademark owners to argue their case as Virtual Worlds would be treated as just a different technological platform.

A challenge also remains in Second Life relating to the accountability for virtual item creation and management (avatar inventory management) to lie with individual avatars. Unlike There.com where the operator of the Virtual World controls the introduction of a virtual item to prevent trademarked and copyrighted materials from being introduced without license or authority, Linden Lab may not be aware of such instances until complaints are made. A not dissimilar situation has arisen in the 2D Internet, where the jewellery store Tiffany accuses eBay Inc. of taking insufficient action to stamp out the transaction of pirated Tiffany goods. In the situation of Second Life, the issue is further complicated due to the potential conflict in accountability – the accountability of the platform operator (Linden Lab), the virtual mall owner (which may be any avatar, virtual business or real life business), and the retailer of the virtual item.

Issues also exist regarding the creation of virtual buildings and locations that resemble real world buildings and locations. Do owners, designers and architects of real world buildings and locations have a right to prevent their work from being replicated or simulated in Virtual Worlds? The unauthorised and often blatant reproduction of real world architecture may mislead avatars to perceive that an association exists between owners of the real world design and owners of the virtual reproduction. The unauthorised use and reuse of intellectual property in Virtual Worlds will remain a controversy due to the heavy dependence of the virtual economy on trading of virtual items, and the creative nature of Second Life activities.

Frauds, Scams, and Ethics in Virtual Worlds

Ethical issues in Virtual Worlds are almost due to the limitless opportunities for real world activities to be mirrored in Virtual Worlds. Apart from copyright infringement and privacy issues, opportunities exists for frauds, scams, deception and phishing attacks, theft of virtual items, and intrusion to virtual lands in Virtual Worlds.

The Real Money Trading ability of Second Life may be exploited by fraudulent monetary transactions and for small scale money laundering, or for speculative currency trading activities. The lack of governance of virtual business leaves open avatar consumers to unethical scams and pyramid schemes. The absence of a security force and law enforcement agency leaves open opportunities for scams and frauds to propagate quickly, and violent virtual fights between avatars. These highlight the weakness of existing real world legislative framework in addressing violation of various rights in Virtual Worlds.

Of particular interest is the possibility for malicious use of the permission request system in Second Life. A virtual item that is advertised as a freebie may incur hidden charges, or ongoing charges, once the transaction has been initiated. The permission request system that is frequently used to enable avatars to be animated by dance sequence could also lead to the hijacking, misuse, misuse of avatars, much like the effects of phishing attacks in the traditional 2D Internet.

CONCLUSION

This paper discusses the broad implications of privacy and intellectual property protection in Virtual Worlds, and the nature of fraudulent activities emerging in Virtual Worlds. For Virtual World users and stakeholders, the most effective weapon and protection against these modern challenges lies in equipping themselves with up-to-date knowledge. Apart from that, the tried and tested common sense believe that “if something is too good to be true, it is most probably not true”.

Security and ethical issues in Virtual Worlds represent a major challenge for Virtual World users and stakeholders. As evidenced by IBM’s introduction of “IBM Virtual World Guidelines”, early adopters of Virtual Worlds addressed these challenges by introducing policies and guidelines to help employees adopt the new technology. Law enforcement agencies, government regulators and lawmakers, as well as researchers play important roles in establishing structures and frameworks in Virtual Worlds, especially in providing guidance on how to weed out anti-social activities in Virtual Worlds, and on how to maintain the social stability Virtual Worlds. In balancing a delicate balance between restriction of innovation and freedom of users against the security and safety of users, future research projects on Virtual Worlds should address current gaps in knowledge in Virtual Worlds by analysing issues such as technical mechanisms against security breaches in Virtual Worlds, the social aspect of Virtual World security threats, and the issue of governance and regulation of business on new technological platforms.

REFERENCES

Automotive Portal (2007) “Mercedes-Benz launches integrated marketing campaign for the new C-Class” 19 March, URL: <http://www.automotportal.com/article/mercedes-benz-launches-integrated-marketing-campaign-for-the-new-c-class> [Accessed 2 December 2007]

Balkin, J. M. (2004) “Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds” Virginia Law Review, Vol. 90, No. 8, pp. 2043-2098.

- Barnes, B. (2007) "Web Playgrounds of the Very Young" New York Times, 31 December, URL: <http://www.nytimes.com/2007/12/31/business/31virtual.html> [Accessed 1 January 2008]
- BBC News (2006) "Worm attacks Second Life world" Technology, 20 November, URL: <http://news.bbc.co.uk/1/hi/technology/6164806.stm> [Accessed 23 December 2007]
- Business Week (2006a) "My Virtual Life" Business Week, 1 May, URL: http://www.businessweek.com/magazine/content/06_18/b3982001.htm [Accessed 14 December 2007]
- Business Week (2006b) "Palmisano Gets A Second Life" Business Week, 20 November, URL: http://www.businessweek.com/magazine/content/06_47/b4010068.htm?chan=tc&chan=technology_technology+index+page_today's+top+stories [Accessed 14 December 2007]
- Business Wire (2007) "Gartner Says 80 Percent of Active Internet Users Will Have A 'Second Life' in the Virtual World by the End of 2011" URL: http://www.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20070424006287&newsLang=en [Accessed 14 December 2007]
- Castronova, E. (2005) *Synthetic Worlds: The Business and Culture of Online Games*, The University of Chicago Press, Chicago, USA.
- Chatham, R. (2007) "Games for Training" *Communications of the ACM*, Vol. 50, No. 7, pp. 36-43.
- Clark, J. (2007) "Oh, the places you'll go — on the Internet" USA Today, 14 June, URL: http://www.usatoday.com/travel/news/2007-06-14-second-life_N.htm [Accessed 3 December 2007]
- Dibbell, J. (2006) *Play Money*, Basic Books, New York, USA.
- Edery, D. (2006) "Reverse Product Placement in Virtual Worlds" *Harvard Business Review*, Vol. 84, Iss. 12, p.24.
- Forrester (2008) "Getting Real Work done in Virtual Worlds" Executive Summary, 7 January, URL: <http://www.forrester.com/Research/Document/Excerpt/0,7211,43450,00.html> [Accessed 8 January 2008]
- Ginko (2007) Ginko Financial Annoucement, URL: <https://ginkofinancial.com/> [Accessed 15 December 2007]
- Grimmelmann, J. (2004) "Virtual Worlds as Comparative Law" *New York Law School Review* Vol. 49, pp. 147-184.
- Harvard University (2007) "E-4 Virtual Worlds" URL: <http://www.eecs.harvard.edu/~nesson/e4/> [Accessed 16 December 2007]
- Hemp, P. (2006) "Avatar-based Marketing" *Harvard Business Review*, 84 (6), pp. 48-57.
- Hutcheon, S. (2007) "Jitters in Second Life as Bank Shuts Doors" *Tech*, Sydney Morning Herald, 10 August, URL: <http://www.smh.com.au/news/web/jitters-in-second-life/2007/08/10/1186530581488.html?page=fullpage#contentSwap1> [Accessed 31 December 2007]
- LaPlante, A. (2007) "Second Life Lessons: Cisco, IBM Pace Corporate Push Into Virtual Worlds" *Information Week*, 3 February, URL: <http://www.informationweek.com/news/showArticle.jhtml?articleID=197001839> [Accessed 16 December 2007]
- Lemos, R. (2006) "Second Life plagued by Grey Goo attack" *The Register*, 24 November, URL: http://www.theregister.co.uk/2006/11/24/secondlife_greygoo_attack/ [Accessed 23 December 2007]
- Lofgren, E., and Fefferman, N. H. (2007) "The Untapped Potential of Virtual Game Worlds to Shed Light on Real World Epidemics" *The Lancet Infectious Diseases*, Vol. 7, Iss. 9, pp. 625-629.

- Kirkpatrick, D. (2007) "It's Not A Game" CNN Money, URL: http://money.cnn.com/magazines/fortune/fortune_archive/2007/02/05/8399120/ [Accessed 15 December 2007]
- Laughlin, D. (2007) "NASA's Exploration of Immersive Environments as Learning Tools" presentation slides, 6 November, URL: <http://www.slideshare.net/naypinya/nasa-use-of-immersive-environments/> [Accessed 23 December 2007]
- Lazarus, D. (2006) "Real fear in virtual world" SF Gate, 15 September, URL: <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/09/15/BUGE9L5JM51.DTL&type=tech> [Accessed 23 December 2007]
- Moore, M. (2007) "French Politics in 3-D on Fantasy Web Site" Washington Post, 30 March, p. A01, URL: <http://www.washingtonpost.com/wp-dyn/content/article/2007/03/29/AR2007032902540.html> [Accessed 23 December 2007]
- Reuters (2006) "Ginko Financial – Pioneer or Pyramid?" URL: <http://secondlife.reuters.com/stories/2006/10/15/ginko-financial-pioneer-or-pyramid/> [Accessed 15 December 2007]
- Reuters (2007a) "HBO buys machinima film created in Second Life" 4 September, URL: <http://secondlife.reuters.com/stories/2007/09/04/hbo-buys-machinima-film-created-in-second-life/> [Accessed 23 December 2007]
- Reuters (2007b) "Congressional Democrats' agenda gets SL stage" 2 January, URL: <http://secondlife.reuters.com/stories/2007/01/02/congressional-democrats-agenda-gets-sl-stage/> [Accessed 23 December 2007]
- Reuters (2007c) "Residents threaten lawsuit to force landbot ban" 24 October, URL: <http://secondlife.reuters.com/stories/2007/10/24/residents-threaten-lawsuit-to-force-landbot-ban/> [Accessed 23 December 2007]
- Reuters (2007d) "SL Business Sues for Copyright Infringement" 3 July, URL: <http://secondlife.reuters.com/stories/2007/07/03/sl-business-sues-for-copyright-infringement/> [Accessed 23 December 2007]
- Reuters (2008a) "SL Banks Scramble for Survival Ahead of Deadline" URL: <http://secondlife.reuters.com/stories/2008/01/17/sl-banks-scramble-for-survival-ahead-of-deadline/> [Accessed 17 January 2008]
- Reuters (2008b) "Live from the World Economic Forum in Davos" URL: <http://secondlife.reuters.com/stories/2008/01/16/live-from-the-world-economic-forum-in-davos/> [Accessed 17 January 2008]
- Reuters (2007xx) "Eros asks for default judgment after Leatherwood misses deadline" URL: <http://secondlife.reuters.com/stories/2007/11/15/eros-asks-for-default-judgment-after-leatherwood-misses-deadline/> [Accessed 15 December 2007]
- Robins, S. (2007) "Immersion and Engagement in a Virtual Classroom: Using Second Life for Higher Education" Presentation at ELI Meetings, 27 March, URL: <http://www.educause.edu/ir/library/pdf/ELI07216.pdf> [Accessed 23 December 2007]
- Rose, F. (2007) "How Madison Avenue is Wasting Millions on a Deserted Second Life" Wired Magazine, Issue 15.08, URL: http://www.wired.com/techbiz/media/magazine/15-08/ff_sheep [Accessed 15 December 2007]
- Second Life (2007) "Wagering In Second Life: New Policy" *Official Linden Blog*, 25 July, URL: <http://blog.secondlife.com/2007/07/25/wagering-in-second-life-new-policy/> [Accessed 16 December 2007]

- Second Life (2008a) "Second Life | Economic Statistics" 23 January, URL: http://secondlife.com/whatis/economy_stats.php [Accessed 23 January 2008]
- Second Life (2008b) "Second Life Key Metrics through December 2007" URL: http://www.google.com/url?q=http://static-secondlife-com.s3.amazonaws.com/economy/stats_2007_final.xls&sa=D&usg=ALhdy2_T3vVJxn4K36-uCl3iyCHLdl96eQ [Accessed 1 January 2008]
- Second Life Herald (2007) "The Greed Shepherd" 9 April, URL: http://www.secondlifeherald.com/slh/2007/04/the_greed_sheph.html [Accessed 23 December 2007]
- Simmons, C. (2007) "Sweden opens virtual embassy 3D-style" Sweden.se: The Official Gateway to Sweden, 30 May, URL: http://www.sweden.se/templates/cs/Article_16345.aspx [Accessed 23 December 2007]
- Stott, D. (2007) "Attending medical school in virtual reality" Student BMJ, December, URL: <http://student.bmj.com/issues/07/12/news/431.php> [Accessed 23 December 2007]
- Sydney Morning Herald (2005) "Online gamer killed for selling virtual weapon" URL: <http://www.smh.com.au/news/World/Online-gamer-killed-for-selling-virtual-weapon/2005/03/30/1111862440188.html> [Accessed 15 December 2007]
- Terdiman, D. (2006) "Virtual magnate shares secrets of success" News.com, 20 December, URL: http://www.news.com/Virtual-magnate-shares-secrets-of-success/2008-1043_3-6144967.html?tag=item [Accessed 23 December 2007]
- Thompson, C. (2006) "The Game within the Game" Wired, 22 May, URL: <http://www.wired.com/gaming/gamingreviews/commentary/games/2006/05/70945> [Accessed 23 December 2007]
- Timson, L. (2008) "Watch and Learn" The Age – Tech, 7 January, URL: <http://www.theage.com.au/news/web/watch-and-learn/2008/01/06/1199554469090.html?page=fullpage> [Accessed 7 January 2008]
- University of Nottingham (2007) "No escape from the bullies" 31 May, URL: <http://research.nottingham.ac.uk/NewsReviews/newsDisplay.aspx?id=340> [Accessed 23 December 2007]
- Vodafone (2008) "What is Vodafone InsideOut?" URL: <http://secondlife.vodafone.com/what.aspx> [Accessed 1 January 2008]
- Wagner, M. (2007) "Using Second Life as a Business-to-Business Tool" Information Week, 26 April, URL: http://www.informationweek.com/blog/main/archives/2007/04/using_second_li_2.html [Accessed 15 December 2007]
- WEF (2007) "World Economic Forum Annual Meeting 2007 – Enlarging the Davos Conversation" URL: <http://www.weforum.org/en/media/Latest%20Press%20Releases/AM07DavosConversation> [Accessed 14 December 2007]

COPYRIGHT

C.Y.Lee ©2008 The author assigns the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors

Designing Ethical Systems for Online Systems

Shona Leitch and Matthew Warren

School of Information Systems, Burwood,
Deakin University, Australia,

E-mail: shona@deakin.edu.au and mwarren@deakin.edu.au

Abstract

Ethics is an important element in all aspects of Information Systems (IS), from the design, operation and delivery of such systems. Most research has focused upon traditional IS system design and the associated ethical issues.

There are many aspects of ethics that can impact the design and operation of Information Systems, but online system design is often overlooked. The paper will focus upon a design approach that allows for the design on online systems and considers the ethical issues. The approach was developed and validated in regards to a tertiary environment.

Keywords: Online design, Ethics, framework.

Introduction

The internet and internet based information systems have a global impact upon business and society, but has this impact had an impact upon the design of information and especially the ethical issues. Much of the research performed over the past two decades regarding requirement elicitation for software systems has been focused primarily on the development, implementation and evaluation (Coulin and Zowghi, 2005), on what can be assumed as traditional IS systems, this does raise the question, what about online IS systems?

One concern that needs to be considered is that the 'systems' part of an 'information system' represents a way of seeing the set of interacting components, such as:

- People (e.g. systems analysts, users)
- Objects (e.g. computer hardware devices)
- Procedures (e.g. those suggestions made in an IS development methodology)
(Avison, 1999)

Often in systems design, the developers focus on the objects, i.e. making the most technologically advanced system. In the case of this paper, this poses a problem, since we are focusing upon people and particularly in an educational context. The reason for focusing upon an educational example was:

- Online learning systems are complex systems and have to fulfil needs for a magnitude of different users;
- Online learning systems are an example of a system where user focused design is a major consideration e.g. student focused;
- The users of online learning systems are varied group of users e.g. on campus and off campus, local and international students, various ages, etc.

The authors have previously defined a conceptual framework for the design of E-commerce systems (Leitch and Warren, 2002), but wanted to build upon this research to deal with the complexity of online learning systems.

The aim of the research was to produce a method which allow for the design of online system, this approach would encompasses the needs and requirements of users with that online environment. This approach would allow the consideration of ethical issues in the design of such a system.

Implementation of Approach

Deakin University is one of Australia's largest universities (Deakin University, 2007), with five campuses located in Melbourne, Geelong and Warrnambool. It was established in 1974 with one campus located in Geelong. Deakin University was one of the first Australian universities to introduce off-campus learning, first through traditional paper methods and then through Internet technologies. Since 2004, all new undergraduate students have been required to undertake at least one wholly online unit as a part of their degree (Deakin University, 2007), and most units have an online teaching and learning presence. Deakin University currently uses software called Deakin Studies Online (DSO) a part of the WebCT brand of software. This software is used in almost every unit at Deakin University with a "required" amount of information (unit guide) to be provided to students, however most units have a much wider DSO presence, supplying various learning materials, lectures, tutorials, discussions etc.

The authors developed the method - MEAD (Method for Educational Analysis and Design) which could be used for the design of on-line systems, focusing upon user requirements. The MEAD method was based upon Soft Systems Methodology (SSM) (Checkland, 1981). This allowed for the use of a number of key mechanisms such as the use of rich pictures to incorporate the users of a system, as well as providing an easy to understand and relate to method of eliciting and discussing information between the designers and other stakeholders.

The issues of ethical design can be resolved by ensuring that users are key stakeholders in the design of the systems that they will be using. The following describes the implementation of the MEAD method:

Stage 1 and 2

Stage 1 requires that there is recognition that there is an issue with the current online teaching and learning system and therefore some action is required to improve the situation. Usually there is at least one person that recognises the possible problem situation and takes action to improve it. In the case of the online teaching and learning system, this is likely to be an academic staff member who has been informed by students as to problems or limitations of the current system, or has noted through their own teaching, problems with the current system in terms of its design or lack of content and functionality.

In this case of this practical application informal student comments and the staff member's awareness of issues and limitations were the initiation for an investigation into the situation.

The work completed in this stage of the MEAD method was a combined effort guided by the designer but with a large amount of input and consensus by focus group participants.

Data was collected through a survey, gauging student's opinions and attitudes to numerous areas of teaching and learning online at Deakin University. The responses were collated and used to form a consensus opinion as to their attitudes towards these elements. These opinions were then used to create the initial rich picture and problem themes and used within the next stage of the method in the focus group sessions.

Focus groups are very similar to interviews except they are conducted in a group rather than just with an individual participant. Generally, like an interview, the researcher has constructed some basic broad questions for the facilitator to use in encouraging and eliciting discussion in the group. The facilitator helps the group understand their objectives and moderate the discussion without taking a

particular position (Greenbaum, 2000). These focus group interviews are an effective method for bringing together a group of people in a similar situation to discuss their attitudes and opinions to a particular issue (Kumar, 2005).

The first focus group was conducted with a group of students from Deakin University, Australia, who indicated in the returned questionnaire that they were willing to be interviewed. From this list a sample of students were selected. The first was a group discussion of students' attitudes, experiences and opinions of Online Teaching and Learning systems (specifically DSO).

Discussion on the positive and negative aspects of online learning systems layout, content and design took place.

The final major part of the focus group session involved the presentation of a Rich Picture (Checkland, 1981) and the associated Problem themes and were offered up for discussion, a sample rich picture from the validation process can be found in figure 1. Students were asked to comment on each theme and identify any other problems that had not been identified.

The outcome of the first focus group session was to be able to validate and update the rich picture and problem themes that were developed from the survey responses. This stage also identified a number of ethical issues that the students identified, these will be discussed later in the paper.

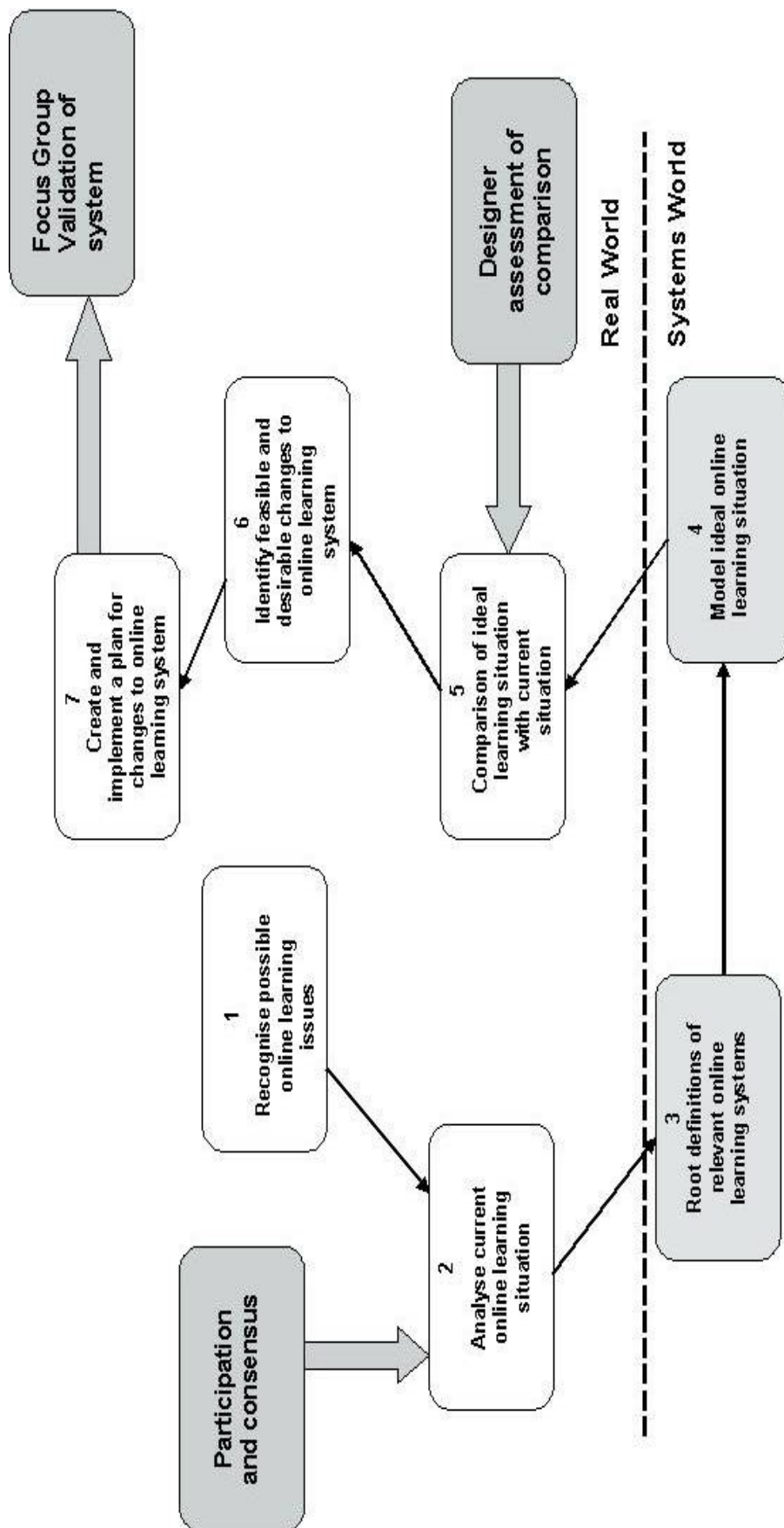


Figure 1 – MEAD Method for the Analysis and Design of Online Teaching and Learning Systems

Stage 3 and 4

These outcomes allowed the researchers to proceed to stage 3 of the method and formulate the SSM root definitions and conceptual models of the ideal online teaching and learning situation.

Stage 5

When reaching stage 5 of the method (comparing the ideal situation with the current situation) a online teaching and learning designer from Deakin University was approached and an interview was conducted, during which the researchers models were discussed and feedback was given by the designer. This feedback was then included in the models before the comparison was conducted.

Stage 6

From the research that has been conducted in the application of this method (from focus group sessions, questionnaire feedback and analysis using the method) there are a number of changes to online teaching and learning system at Deakin University that have been discussed and proposed by the researcher, the participants and the e-learning designer.

Within this stage another area to be assessed was the limitations of Technology involved. The limitations of the online teaching and learning software (DSO) used by Deakin University had to be addressed. WebCT the development company that produced DSO provides a generic standardised package, which is then adapted for use at individual institutions. Even with Deakin University, different templates and styles are used within different Faculties. Some of the limitations faced when developing the DSO example site included:

- Limited selection of integrated communication tools;
- No standard method for social interaction;
- Database style of DSO (would be difficult to alter);
- Overall style of DSO site.

Stage 7

The feasible changes that were identified through the SSM analysis were then applied to the specific online teaching and learning system that is used at Deakin University. Along with these feasible changes the specific opinions of the focus group participants (and the survey participants) were also applied to the design and the content inclusions.

A second focus group session was conducted; the participants where presented with the example online teaching and learning system that was produced from the “feasible and desirable changes” that were identified in stage six of the method. This part was presented in the style of a walkthrough, showing the participants the different elements and features that had been included, this included content ideas as well as some different layouts.

Ethical Outcomes

The MEAD method as well as being a user focused design approach, also allows for the consideration of ethical issues. The use of focus groups at stage 2 of the MEAD method allows for ethical considerations to be discussed. In terms of the validation process of the MEAD method, the following ethical considerations were identified:

- Implement a social networking and interaction aspect to online teaching and learning;
- Provide more useful information resources;
- Provide varied resources for students that include both audio, visual and interactive mediums;

- Larger Internet download limit for student to access materials suggested by staff on DSO for students to access;
- Wholly online units to be removed from the curriculum and online teaching and learning to be used as a supplemental resource to traditional face-to-face teaching;
- Online questions posed by students to be replied to by a staff member within twenty-four hours;
- Lecture theatres to be fitted with adequate power outlets for students to be able to use laptops to take notes during classes (outside the realm of online teaching and learning system design);
- Users (students) of online teaching and learning systems should have input into the design of said system.

As Stage 7 of the MEAD method, through the second focus group the feasibility of the considerations were discussed.

Without the user focus of MEAD, these ethical considerations would not have been highlighted and considered as part of the design process.

Conclusion

This MEAD method has been developed as an alternate way of developing online learning systems. The approach allows for high levels of user involvement at specific stages of the method (stage 2, 5 and 7 has the most user participation). This is to endeavour to improve the planning and analysis of online learning systems and try to achieve a system that works for the user and also considers ethical issues as well.

The application of this MEAD method took place in a tertiary institution (Deakin University) in Australia but the method could be applied within other tertiary institutions or used to design business online systems.

References

- Avison, P. & Fitzgerald, G., (1999) " *Information Systems Development: Methodologies, Techniques and Tools*". McGraw-Hill, UK.
- Coulin, C and Zowghi, D (2005) What do Experts think about elicitation? – A state of practice survey, Proceedings 10th Australian Workshop on Requirement Engineering, Melbourne, Australia, ISBN 1-74156-029-2.
- Checkland (1981) "Systems Thinking, Systems Practice", Wiley, Chichester.
- Deakin University (2007). About Deakin. <http://www.deakin.edu.au/about/history.php> [accessed 10/10/2007]
- Greenbaum, T. L. (2000). Moderating Focus Groups: A Practical Guide for Group Facilitation. Sage Publications Inc.
- Kumar, R. (2005). Research Methodology. Sage Publications Ltd.
- Leitch, S and Warren M.J (2002) Designing Ethical Systems for Electronic Commerce, 3rd Australian Institute of Computer Ethics Conference, Sydney, Australia.

COPYRIGHT

Leitch and Warren ©2008 The authors assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.

Young People and the Internet – What is the solution?

Shona Leitch and Matthew Warren,
School of Information Systems,
Deakin University,
Melbourne, Victoria, Australia, 3137.

Abstract

New Technology is an important aspect of society, but the impact of new technology has changed the way in which society can view and deal with many traditional issues. Young people have access to the internet and in many cases are left to their own devices and free to explore a variety of sites via the internet, even if the content is unsuitable.

The paper will explore the issue of how to control the internet and how young people deal with the Internet. The paper will explore the issues of government and also school in helping young people with these new challenges.

Keywords

Australia, Internet, content and control.

Introduction

The Internet was initially designed for military purposes and academic institutions, that was until the creation of the World Wide Web in 1990 and the release of Mosaic in 1993, the first piece of software to allow “point and click” internet perusal (Hird, 2000), the rest is history.

With the growth of the Internet, controlling the Internet has become an increasing problem due to a number of factors including its continued popularity (especially with children), lack of global boundaries, policing and censorship. The lack of control of over the Internet, has been one of the reasons why the growth. This paper will look primarily at the issues surrounding young people and their use of the Internet, how it is changing their day to day lives and the possible solutions to an ever increasing problem.

Young Peoples use the Internet for a variety of purposes, both educational and for entertainment. There has been recent data collected on this usage issue by the Australian Bureau of Statistics (2006a). This information is summarised in Figure 1.

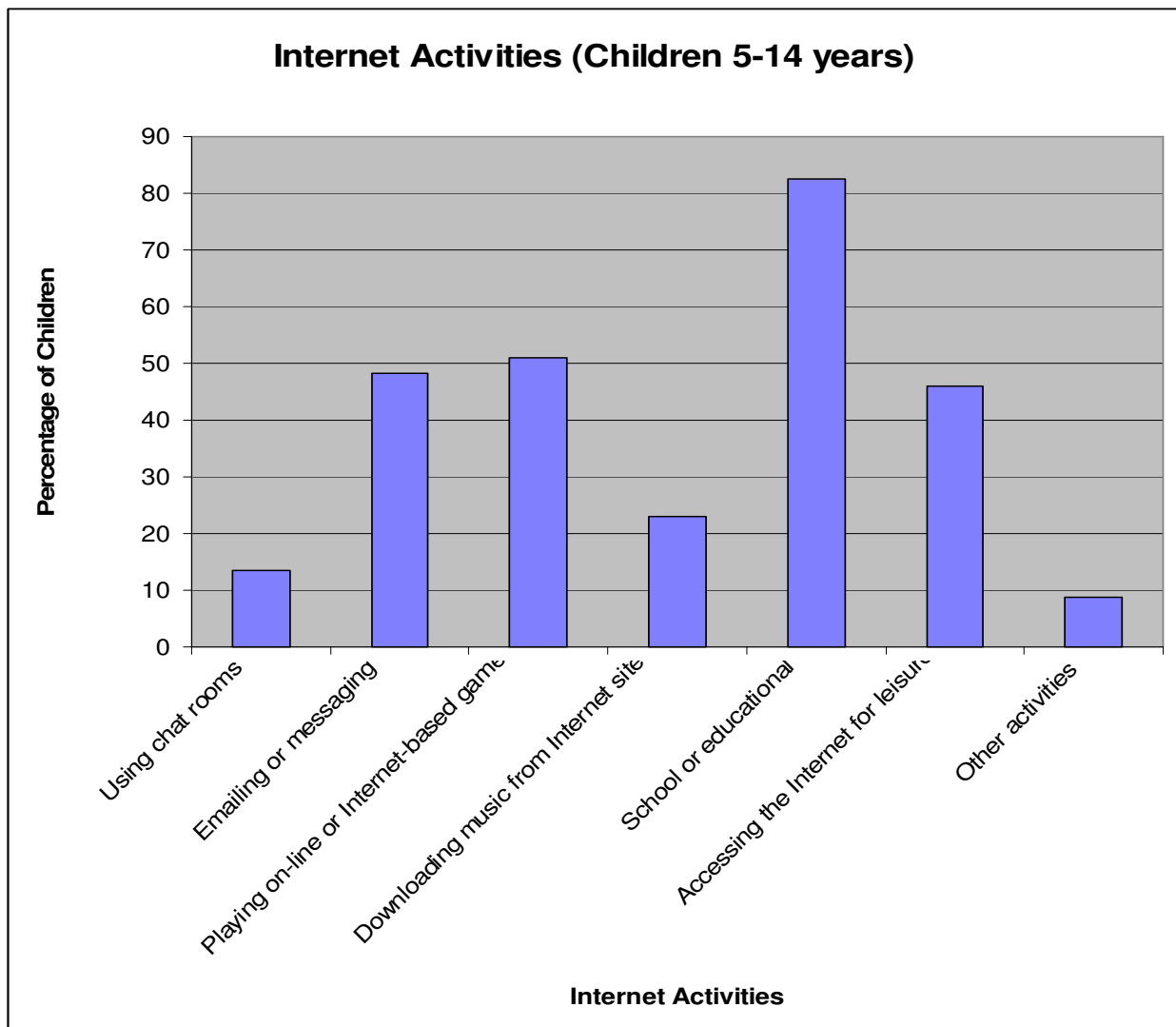


Figure 1: Children's Internet Activities (ABS, 2006a)

The statistics shown in Figure 1 clearly show that children are using the Internet for educational purposes, most likely, research for assignments, however 50% are also playing online based games, and perhaps the most worrying nearly 50% are using e-mail and instant messaging, which is often reported as a method predators use to gain access to children online.

The Australian Bureau of Statistics (2006b) shows that almost 76% of children aged between 9 and 11 years old have accessed and used the Internet.

Age group	Have accessed the Internet (%)
5-8	37.7
9-11	75.6
12-14	88.7

Table 1: Percentage of children accessing Internet content (ABS, 2006b)

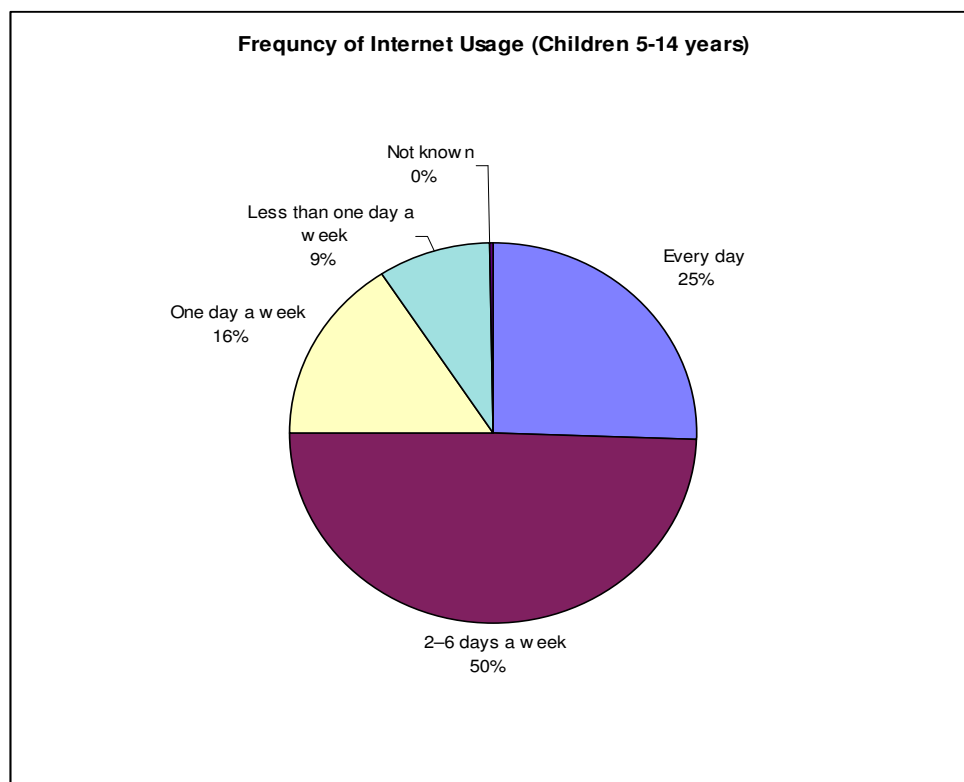


Figure 2: Frequency of Internet Usage. (ABS, 2006b)

We also know that at least 25% of children are accessing the Internet daily (see Figure 2) with 75% “going online” at least twice a week (ABS, 2006b), which could increase the potential risks that young people face on-line.

The Australian Federal Government’s NetAlert agency has identified a number of key issues related to children and the Internet and have identified the following as items that are “potentially addictive for children” (NetAlert, 2007).

- Instant Messaging and Chat;
- Online Gaming (e.g. WoW, Runescape, NeoPets etc.);
- Social Networking (e.g. My Space, Bebo etc.);
- Viewing risky content (such as pornography);
- Downloading files (especially in Peer-2-Peer networks).

Australian Government Policy

Within Australia both the Liberal party and the Labour party do not fully understand the Internet. The recent discussion about censoring the Internet reflects that lack of understanding. The Internet cannot be controlled from Canberra. The biggest problem that Australia (as all countries) faces is the fact that the Internet is global and there are no global agreements about its content or control. The Internet contains much positive information but unfortunately it contains so much negative information. This information is distributed freely around the world and this is why all governments need to be involved in its control. Governments will need to create the equivalent to the United Nations Universal Declaration of Human Rights for instance the “Universal Declaration of Internet Content”. The Internet’s global nature is reflected by the scourge of child pornography and the deaths caused by

Internet suicide chat rooms especially in Japan and South Korea. None of these major issues can be solved by Australia alone taking a stance, it will require global co-operation and global enforcement.

As mentioned previously Australia cannot control the Internet or its content, the government cannot expect Australian Internet Service Providers to track every transaction that they process and can we expect NetAlert to solve the problems of the Internet with increased funding or new software filters. The filter was offered free to families earlier this year by the government so they could block black-listed material and protect their children. But recent reports that the Federal government's anti pornography filter for the Internet had been hacked by a Melbourne teenager. The problem is that technological solutions cannot solve all problems of Internet protection and this case shows how technology can be bypassed and how filters cannot offer 100% protection. There has to be alternatives to technical solutions.

The political parties should look at new methods to protect the Internet, measures that could be adopted, could include:

- global co-operation to remove pornography;
- teaching computer ethics in school – to establish standards for young people about acceptable behaviour on the Internet;
- increased funding for bodies such as NetAlert to give up to date advice about the risks of Internet content;
- ongoing funding for non-technical protection initiatives including awareness campaigns;
- parents educating themselves about the problems associated with the Internet.

Since the general election and the change of government took place within Australia, one of the new key government policies is to try and censor the Internet within Australia via the use of Internet Service Providers controlling the content of the Internet (Heywood, 2007, Syvret, 2008), only time will tell if this strategy proves to be successful.

Schools and Internet

Schools have a major role in protecting young people against the dangers of the Internet by teaching computer ethics. Computer ethics is a set of moral principles that govern the behaviour of a group or individuals in relation to technology and in this instance in relation to the Internet. A major problem is the way that computer ethics should be taught, a computer ethics unit by itself would be very dull to young people and they could view computer ethics in a negative manner. A more effective way to teach computer ethics is to embed aspects in other subjects. In the UK several schools teach citizenship studies, teaching about appropriate behaviour as an adult, computer ethics could be linked to subjects or discussions relating to this appropriate behaviour. Young people could also keep reflective diaries about their experiences on the Internet and these could be used as a tool as part of classroom discussions.

It is important that computer ethics should be taught at all levels of education, young people could be taught about the issues of chatting online, information they should not share online, the problems of cyber bullying and how deal with this issue and the ethical problems of piracy and hacking.

One of the problems society faces, is that young people are now brought up with easy access to the Internet, they chat socially, they have personal blogs, they download music and movies from the internet, they exist in virtual worlds such as second life, etc. The problem is that young people may have greater knowledge of technology than their parents or teachers, this poses unique issues.

By teaching computer ethics at all schools it will help to establish standards for young people about acceptable behaviour on the Internet. These personal standards will help them in all aspects of their adult life.

Within Australia, parents should be very concerned about young people using the Internet, the type of information that they can view, as well as the type of people who may contact them via this medium. But parents have the ability to do something about it, raising awareness with their children about appropriate Internet behaviour or buying technology to block unsafe sites.

The government would be better placed ensuring that computer ethics is taught to young people, this could be a low cost solution to a massive problem. A technology solution to controlling the Internet simply cannot succeed. As a society we have to accept that the Internet will be with us forever and it is going to pose many social problems for Australian society as a whole in particular the young people of Australia.

Conclusion

The solution to controlling the Internet in relation to children's access, usage and reliance on it lies in more than just a technical solution. It is necessary for all people involved to assert control. Parents in taking a proactive solution to being aware of what their children are using the Internet for and becoming more Internet and technologically savvy. Schools need to teach children computer ethics and promote a healthy understanding of the Internet, the positive and the negative aspects. And finally governments need to use appropriate policies to regulate and oversee, but at what cost to the individual.

References

Australian Bureau of Statistics (ABS) (2006a), "Table 27. COMPUTER AND INTERNET ACTIVITIES, Characteristics of children",
[http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/76C7FB8644F18A71CA2572440077DCA8/\\$File/49010_table27_apr%202006.xls](http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/76C7FB8644F18A71CA2572440077DCA8/$File/49010_table27_apr%202006.xls), [accessed 20/05/07].

Australian Bureau of Statistics (ABS) (2006b), "Table 30. HOME INTERNET USAGE, Activities and usual frequency in the past year",
[http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/97C936F20A966FF0CA2572440077E136/\\$File/49010_table30_apr%202006.xls](http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/97C936F20A966FF0CA2572440077E136/$File/49010_table30_apr%202006.xls),
[accessed 20/05/07].

Heywood, L. (2007) Onus on providers to clean up web content, News.com.au
<http://www.news.com.au/story/0,23599,22989028-421,00.html>
[accessed 1/1/08].

Hird, A., (2000), Learning from Cyber-Savvy Students: How Internet-Age Kids Impact Classroom Teaching, Stylus Publishers.

NetAlert (2007), What can children become addicted to online?, <http://netalert.net.au/03784-What-can-Children-Become-Addicted-to-Online.asp>, [accessed 12/05/07].

Syvret, P (2008) Nanny Rudd censors the internet, News.com.au,
<http://www.news.com.au/couriermail/story/0,23739,22990520-27197,00.html>
[accessed 1/1/08].

COPYRIGHT

Leitch and Warren ©2008 The authors assign the Deakin University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to Deakin University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.