Conference Proceedings of

A*i*CE 2005

Geelong, September 26th, 2005.

Fourth AUSTRALIAN INSTITUTE OF COMPUTER ETHICS CONFERENCE

Edited by:
Matthew Warren
ISBN 1 74156 021 7

Proceedings of

A*i*CE 2005

Edited by
Matthew Warren
ISBN 1 74156 021 7

Published by the School of Information Systems, Deakin University, Geelong, Victoria 3217, Australia.

All papers published in the conference proceedings have been blind refereed by at least two of the A*i*CE 2005 **Organising** committee.

Welcome

The A*i*CE2005 conference follows on from the highly successful initial AICEC99, AICE2000 and AICE2002 conferences. This conference looks at the continued development of Computer Ethics within Australia taking into account the issues of the 21st Century.

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 within the 21st Century.

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

A*i*CE 2005 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

Ethics Across National Borders: How Can We Cope With Actual Problems?

John Weckert
Centre for Applied Philosophy and Public Ethics
Charles Sturt University, Australia.

1 INTRODUCTION

Because of the Internet, national borders are becoming transparent. This is creating some interesting, and urgent, ethical problems given the often conflicting moral and legal customs and structures in different countries. This paper will examine some of the ethical issues that arise in three recent cases. These issues are not completely new of course. As long as there has been international trade and people have been visiting foreign climes there have been culture clashes. The Internet did not create them and even now they occur quite independently of the Internet, for example in the recent and on-going drug cases involving Australians in Indonesia where different legal systems and different sentences cause frictions and misunderstandings. What is different though is that as a result of the transparency of international borders in the on-line environment issues occur in ways that they did not before. Without travelling I can be confronted by an alien culture or foreign laws, or when I travel I might be in trouble for something that I did at home that was not illegal there.

2 CASES

Case one - defamation: The High Court of Australia ruled that a defamation case could be heard in the State of Victoria even though the offending material was on a server in the United States. A prominent Australian businessman, Joseph Gutnik, argued that the case should be heard in Victoria on the grounds that that is where the material was read and his reputation harmed. The company, financial publishers Dow Jones, argued that because the material was on a server in the US, that is where the trial should be held (BBC, 2002).

Case two – giving offence: An Australian citizen, Friedrick Töbin, maintained a web site, on an server in Australia, that contained material denying the holocaust in World War Two. This material is undoubtedly very offensive to many, but was at that time legal in Australia. It was however, illegal in Germany, and when visiting Germany Töbin was arrested, not only, it must be said, for the material on his Australian web site. The charge relating to the on-line material was eventually dropped, when a German court ruled that as the relevant website was housed outside Germany the court had no jurisdiction (IJHR, 1999). The Federal Court of Germany has now overturned that decision, stating that there is jurisdiction as the material can be accessed by users in Germany .

Case three – intellectual property: This is really two cases, but they will be treated as two parts of one. 1. A bill before the US House of Representatives that would "give American copyright holders freedom to hack PCs used to illicitly share files over peer-to-peer (P2P) networks, without fear of prosecution or litigation" (Cochrane, 2002). 2. … for educational purposes and to encourage computer usage, we [the Malaysian Government] may consider allowing schools and social organisations to use pirated software (Reuters, 2002).

3 LEGAL VERSUS ETHICAL ISSUES

Given that these three cases all involve legal systems in various countries, it might be argued that the important issues are legal and not moral. That they are legal is not in question, but it does not follow that they are not also moral. In an ideal situation the legal system codifies, to some extent, the moral mores of the society – the moral precedes the legal. The moral should also precede the legal in interactions between countries. The situation is of course a little different, because there is often disagreement about what is moral in these cases, and when attempts are made to develop a legal framework, these differences will almost certainly come to the fore. That there are these differences is often taken as evidence that moral values are relative to a particular culture and that it is pointless to talk of object or absolute values because

none exist. If this is so then it is a hopeless task to try to find common moral ground on which to build international laws. This moral relativist position however, is not as strong as it superficially looks, and in a way it would be strange if it were. Human beings are all basically the same. We require the same things to sustain life and the same sorts of things give us pain and pleasure. James Moor argues that there are certain core values that all people have (Moor, p. 66). These are: life, happiness (pleasure) and autonomy. In order to exercise our autonomy we require the *ability* to do various things, the *security* to do them, *knowledge* about doing them, the *freedom* and *opportunity* to do them, and finally the *resources* to accomplish our goals. In order to achieve a good life we require all of these, but different people will not give all of the components the same weightings and therefore conceptions of the good life will be different for different people, but not radically so. Some people place more weight on security while others on freedom, for example, but all want some of each. The argument here is not that finding the common ground between nations and cultures is easy, the differences are important, merely that it is not a hopeless task and can be pursued with a realistic hope of success.

4 ETHICAL ISSUES

A variety of ethical issues are raised by the cases above, and here we will consider in turn, justice and fairness, giving offence, intellectual property and cultural imperialism.

4.1 Justice and Fairness

The first case highlights justice and fairness. We will take justice as being moral egalitarianism, that is, like cases are treated in a like manner. Unfairness arises when like cases are treated differently. 1. It can be argued that it is unfair to be subject to laws in a jurisdiction other than that in which the offending material resides. While in general, ignorance of the law is not a valid defence, one cannot reasonably be expected to be aware of the law in all countries in which one's material may be read on the Internet. It is simply unfair to subject the US defendant to Australian law (Australian defamation law is considerably stricter than US law). 2. It can also be argued that Australian citizens should have the protection of Australian law when in Australia, and not be subject to the jurisdiction of another country. If the US company had won the right for the case to be heard in the US, then in this instance the businessman, even though an Australian citizen in Australia, and harmed in Australia, would have his case dealt with under US law, a situation which also seems unfair. The situation in both cases seems unfair, or unjust, because regardless of the jurisdiction in which the case is tried, one of the parties is disadvantaged relative to the other, and all should be equal before the law.

The second case also hints at unfairness. If material considered legal is on a server in one country, but is considered offensive and is illegal in another where it can be read, should the author of that material be charged with distributing offensive material when visiting that other country? In Töbin's case he knew that the material was illegal in Germany when he visited there, but the general point about fairness remains the same.

4.2 Giving offence

Case Two highlights the thorny issue of giving offence, or offensive material, particularly offensive material on the Internet. In this case the material was especially offensive to some, but not illegal in most places. One question is what, if anything, should be considered so offensive that there is justification in banning it? Some will argue that the offensive nature of material is never a good reason for restricting freedom of speech or expression. But the situation is not always so simple, and the Töbin case illustrates this. It also shows that usual ways of making decisions regarding offensiveness do not transfer well to the Internet context. It is one thing to look to community standards to assess offensiveness, but quite another to assess it on a global scale.

Because this question of giving offence is not given the attention that it deserves, we will look at it a little more closely. Feinberg suggests two conditions which must be satisfied before coercion is justified with respect to offence. One is *universality* and the other *reasonable avoidability*. Of the former he says:

> For offensiveness ... to be sufficient to warrant coercion, it should be the reaction that could be expected from almost any person chosen at random from the nation as a whole, regardless of sect, faction, race, age or sex.

Of reasonable avoidability he writes:

> No one has a right to protection from the state against offensive experiences if he can effectively avoid those experiences with no unreasonable effort or inconvenience (Feinberg, 1973, p. 10).

We will consider these in turn.

The obvious problem with universality in the context of the Internet is that it is too weak to be useful. Given the global nature of the Internet, probably very little will be offensive to all. Ridiculing Christianity would not be universally offensive, as it might be in a Christian country. Mocking a national group will not offend too widely, apart from the members of that group.

A supporter of this universality principle could, of course, happily go along with all of this, and claim that all it shows is that nothing on the Internet should be restricted just on the grounds of offensiveness. (It could be argued though that this is a reasonable criterion when considering restrictions in any one country.)

Feinberg's second principle is reasonable avoidability, and this does have some plausibility. If I am offended by certain Web sites, I can easily avoid them, and consequently there seems to be no good reason why they should be banned on the ground of giving offence. This situation is very different from one where I was confronted by offensive material each time I logged on to the Internet, say by a particular welcoming message or the wording of a prompt or image of an icon. If I am offended by the sight of nude humans (not just pornographic images) on the Internet I seem to have little cause for complaint if I can only access such images via torturous paths punctuated by warnings.

The problem with this is that it is really only plausible in the case of milder offences, actions which are only thought wrong because they offend, and not those which offend because they are thought wrong. If something is found offensive because it is believed wrong, those offended will not be placated by just keeping it away from their eyes and ears, any more than most of us are willing to condone murder which occurs away from us. That it is happening at all is offensive, and this is clearly the situation in the Töbin case.

It might be argued of course that in the Töbin case it is not a matter of offence at all but one of harm. Material of the type in question can incite racial hatred with all that that entails, and while it might also be offence its harmful nature is much more important. This may well be true, but the point here is that standard accounts of offence do not work well in that global context and require rethinking.

4.3 Intellectual property

Case three illustrates quite starkly a dramatic difference in attitudes to intellectual property in different countries. On the one hand there is a country considering using pirated software in its schools, and on the other, a country contemplating enforcing its copyright laws globally. To justify this enforcement, unauthorised copying must really be quite wicked. But is it? Ownership of intellectual property is defended most strongly by those most wedded to capitalism, for the obvious reason that intellectual property is seen as a commodity with monitory value. Not all cultures however, see things this way, and therefore there is a much greater tendency for what we consider intellectual property to be in the public domain, so copying is not seen as a particular evil. Consider the Malaysian example. Suppose that pirated software is used in schools. What is the problem? No other users are deprived of its use, and no-one is loosing any sales because of it. The schools have no money to buy it (or the Government does not have the money to give them), so either they use it without paying, or they do not use it at all. So by copying, they gain and nobody looses. It is not difficult to understand this point of view. It is however, very different from the view of the supporters of the proposed bill in the US, as outlined in the other report. Because of the technology, the US view could be imposed on Malaysia, but should this happen? One argument for the US position is this. If those in developing countries are allowed to freely copy software some of that software, perhaps much of

it, will find its way back to the US and other developed countries and thereby undermine the market in those countries. The copied software that is used in the developing countries might not in itself be a problem, but that resold in the developed countries would be. This argument has plausibility and is also an argument against having different pricing structures for developing countries whereby they could buy software at prices that they could afford. Solving this is difficult, but it is not obvious that the best solution is one that deprives those countries of the use of the software.

4.4 Cultural imperialism

It is not easy to define just what a culture is, nor exactly what constitutes imperialism, so it is not surprising that the phrase "cultural imperialism" is a little unclear. In a recent book on the topic the author refuses to define it at all, arguing that:

> a better way of thinking about cultural imperialism is to think of it as a variety of different articulations which may have certain features in common, but may also be in tension with each other, or even mutually contradictory. One way of putting this is to speak of the *discourse of cultural imperialism* (Tomlinson, 1991, p. 9).

His reason for saying this is that there is no coherence "in the various writings and sayings about cultural imperialism " (Tomlinson, 1991, p. 8). It is not just that there are different interpretations of the thesis, there is no thesis "*there are only versions*" (Tomlinson, 1991, p. 9). Alexeyeva agrees that it is difficult to know what cultural imperialism is, but for a different reason; it is difficult to know what are "native" and what are "foreign" cultural values:

> What is 'native' and what is 'foreign' in present Russia: religiousness or scepticism towards religion? Collectivism or individualism? Respect or disrespect for property rights? (Alexeyeva, 2000, p. 64).

Her second reason is that it is not clear what foreign values are being promoted anyway. For example,

> If computer games – including those available [on the] Internet – are full of violence, does it follow that violence is a cultural value in the countries where the games are produced? (Alexeyeva, 2000, p. 64).

These are all legitimate concerns in discussions of on-line cultural imperialism, but while there may be the problems that she mentions with the concept in Russia, there do seem to be some fairly clear cases of cultural difference, for example in the two cases mentioned earlier.

However, a working definition is required, and here we will accept that in *The Fontana Dictionary of Modern Thought:*

> *Cultural imperialism* may be defined as the use of political and economic power to exalt and spread the values and habits of a foreign culture at the expense of a native culture (Bullock and Stallybrass, 1977, p. 303).

The claim here is not that this *exalting, spreading and supplanting* need be intentional in the sense that the dominant power has any sort of plan to impose its culture on anyone else, let alone a plan to control others. Our interest is in whether or not it *matters* that it is occurring rather than in *why* it is.

Case three illustrates a situation that could be interpreted as a case of cultural imperialism. One report, in the Australian press, says:

> File sharing's global nature means Australians otherwise outside the reach of US authorities will in effect be directly subject to US law. There are no provisions to protect or isolate PCs in other countries. (Cochrane, 2002)

The proposed US law would, it seems make people worldwide subject to US law, regardless of intellectual property laws in their own countries. This does seem to be a clear case where one society is imposing its cultural values on another, but probably without realising that this is what it is doing. It believes that it is upholding a value that is universal, or ought to be. (There is no suggestion that the proposed US bill is directed at Malaysia. The two reports coincidentally came out more or less at the same time.)

5 WHAT SHOULD BE DONE?

Raising the problems is easy, knowing how to solve them justly is not. To solve problems such as that illustrated in Case one, international laws can be established to determine under which jurisdiction defamation cases will be tried, but where the laws of the individual countries differ substantially, it is not clear how the international law can be fair. Perhaps individual defamation laws need to be brought more into line with each other, but this would need to be done in a way that the laws of the stronger were not necessarily imposed on the weaker.

The situation is similar in Case three. All countries could be forced to abide by intellectual property laws as they operate in most Western countries. But it is not clear that this would be just. There is nothing sacred about the notion of intellectual property, and not all societies see it as important. If such laws are enforced this would need to be done in the light of individual societies' customs and their ability to pay.

Case two raises a messier issue. It is obvious that material that is offensive to anyone anywhere cannot be made illegal. There would not be much left to be said. On the other hand, is seems too simple, and rather heartless, to maintain that giving offence should never be taken into consideration. Offensive material can cause distress, and one should avoid distressing others whenever possible. It is less clear here than in the defamation case how international law can help. There is never going to be international agreement on what constitutes offensive material, there are enough problems in getting agreement *within* countries. Perhaps there should be a law that prohibits charging a person in one country for material on a server in another when that person is a citizen of that other country. But even this would not be welcomed by all:

> Expressing concern that the Mannheim court's verdict [in the Töbin case] sets a dangerous precedent, prosecutor Hans-Heiko Klein immediately lodged an appeal. "This is the first time," he said, that "a court in Germany has decided that some things which are said in [sic] Germany on the Internet cannot be subject to German laws. This is a very bad thing. It will undermine our laws which are very important for ensuring that history in Germany is not repeated."[2]

The best solution may be that countries filter out material that they find too objectionable, as some do now. This of course, raises other problems.

These musings indicate that solutions acceptable globally will be difficult to find. But given that the Internet is global, more or less, these problems must be faced. There is no way of avoiding them. And given too that all humans are basically the same it would be surprising if there were not some core moral values that all share, on which to base these solutions.

REFERENCES:

Alexeyeva, Irina, 2000, comment in Langford, Duncan, ed. *Internet Ethics,* London, Macmillan.

BBC 2002, "Australia makes landmark net ruling"
http://news.bbc.co.uk/2/hi/asia-pacific/2560683.stm
Wednesday, 11 December.

Bullock, A. and Stallybrass, O. (eds), 1977, *The Fontana Dictionary of Modern Thought,* London: Fontana Books.

Cochrane, Nathan, 2002, "Hollywood seeks the right to hack", *The Age*, 30 July. www.theage.com.au/articles/2002/07/26/1027497416300.html.

Feinberg, Joel 1973, *Social Philosophy*, Prentice Hall, INC.: Englewood Cliffs, New Jersey, p. 44.

IJHR 1999, "German Court Sentences Australian Holocaust Skeptic [Fredrick Töben] "*The Journal for Historical Review 18,* July/August.
http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html.

Moor, James H. 1999, "Just consequentialism and computing", Ethics and Information Technology 1, 65-69.

Reuters, 2002, “Malaysia ponders pirated software for schools”, 28 July, sg.news.yahoo.com/reuters/nklr250005.html.

Tomlinson, J.,1991, *Cultural Imperialism: A Critical Introduction*, London: Pinter Publishers.

COPYRIGHT

ICT Integrity: Rethinking the Australian Professional Code of Ethics.

Michael Bowern, Charles Sturt University, Australia.
Oliver K. Burmeister, Faculty of Information and Communication Technologies, Swinburne University of Technology; and PhD student, Charles Sturt University, Australia.
Don Gotterbarn, East Tennessee State University; Chair ACM Committee on Professional Ethics, USA.
John Weckert, School of Information Studies, Charles Sturt University, Australia.

Abstract

There have been changes over the last 20 years which affect ICT systems and services. These changes include developments in technology, such as even faster and smaller computers and other digital devices, the convergence of technology, the internet, and operational aspects such as outsourcing. Governments and professional societies have responded to these changes in the media, yet the Australian Computer Society's Code of Ethics has not changed. Perhaps it is time to update it? The functions of the Code include articulating ethical standards of the profession and providing guidance to resolve ethical quandaries. One needs to identify if a code is adequate to address changing practice and technological advances. If a code is inadequate then what can be done to address, consistently, these deficiencies? With the focus on the Australian context, the ACS Code's relationship with international standards and codification of ethics are considered. The issues considered include the lack of specificity, and the absence of a way to decide between ethical principles which may conflict in some situations. Which principles, if any, have a higher priority than others, and why? Further work is needed to identify how the Code of Ethics can best provide moral guidance to ACS members.

Keywords
Codes of ethics, codes of conduct, ACS, ICT ethics, outsourcing, professional societies.

INTRODUCTION

Systems using information and communications technology (ICT) are not produced in an ethical vacuum. The values of many stakeholders are involved. Typically these stakeholders are suppliers, vendors, employees, contractors, trade unions, and clients, and those who are affected by the delivery of the final product. Increasingly, especially in globalisation and offshore issues, professional societies and politicians can also be involved. One way that professional societies address the diversity of values of so many different stakeholders is by requiring their members to adhere to their code of ethics. Major functions of professional codes of ethics include the requirement to articulate ethical standards of the profession; to educate practitioners and the public about ethical obligations; and to provide guidance to resolve ethical quandaries (Anderson et. al., 1993). Philosophical dialogue about alleged difficulty with codes of ethics includes works by Luegenbiehl (1983), Ladd (1995), Fairweather (2001) and Tavani (2004).

There are numerous terms in the literature for professional codes of 'ethics'. In this paper we follow the guidance of the International Federation for Information Processing (IFIP) (Berleur, et. al, 2004), in discussing two types of codes.

The first type, which Berleur et al refer to as the code of 'ethics/conduct', has a set of high level statements, concerning such issues as honesty and integrity. This code governs 'how the person to whom it applies conducts him or herself in an ethical manner' (Berleur, 2004, p 11). To avoid confusion, this type will be referred to as the code of conduct in the rest of this paper.

The second type of code refers to a 'code of practice' for professionals, which 'governs how the person to whom it applies carries out his or her work technically' (Berleur, 2004, p 11). This code includes a set of detailed statements related to the professional's particular occupational environment. These statements of

practice are more specific and more likely to incur change over time, than the conduct statements. That is, the desire for honesty is less likely to change over time, than is the interpretation of the way in which honest dealings in the occupational environment are to function.

Typically, a professional society would define both types of code for its members in a single document, a good example being the Software Engineering Code of Ethics and Professional Practice. This is 'the standard for teaching and practicing software engineering by the ACM and IEEE-CS' (SECEPP,1999). In this paper, reference to a 'code' or a 'code of ethics' means a document which includes both types of code, covering conduct and practice. Other references will be made to a specific type of code under consideration, for example a 'code of practice'.

The problem we address in this paper is one in applied philosophy. Presuming that a professional code of ethics can usefully serve the education and guidance functions, there are three critical questions.

- How can one identify if the changing technology has reduced the ability of a code of ethics for use in ethical assessment? The code is to act as a guide. It should not be subject to frequent change, as each new technology or ICT work process comes along. Yet the inevitability of change in the ICT industry leads one to recognise that certain changes may require a review of a code of ethics, particularly with respect to its code of practice.
- Given a code that no longer meets some of the significant issues, what can be done to consistently revive the ability of the code of practice to serve this function without undermining the existing strengths of the code of conduct?
- For codes which do not specifically distinguish the practice and the conduct elements, how can one modify the practice elements without also modifying the conduct standards?

These concerns are not new. Each professional society has had to grapple with them at one stage or another. IFIP has recently suggested a series of high level guidelines to assess the strengths and weaknesses of codes of ethics (Berleur, 2004). Perhaps these guidelines could also help with the first of the above points, namely to re-evaluate the efficacy of an existing code, once significant change has occurred in the ICT industry?

Rapidly changing technology does have a negative impact on the adequacy of its professional codes; this paper describes that impact, and ways to ameliorate it.

In the ICT industry one has always had to deal with the relationship between ethical assessment and technology. A brief examination of the evolution of ICT professionals' codes will show that at earlier stages modifications were made to the codes to meet technological changes; and a desire to include their expanded sense of professional responsibility and behaviour occasioned by some of these advances. For example, a major revision of the ACS code occurred in 1985, to better accommodate concerns over computer based crime (Coldwell, 1987). Other changes have been made to include an aspirational function.

As mentioned above, many changes to the ICT industry have taken place since the last major revision of the ACS code, 20 years ago. This paper uses outsourcing as an example of a recent change in ICT which could be considered when reviewing the need to change the ACS code.

This paper also briefly examines reasons for modification to the ACM/IEEE ethical standards.

The paper then focuses on changes currently planned and in progress by the ACS. The paper identifies what were perceived as the major ethical shortcomings, and indicates the common elements required to meet the impact of changes in industry practice, in the education and technical functions of the ACS code. These common elements may be used as guidelines in the next generation of ethical code reform.

THE ICT OUTSOURCING DEBATE

Outsourcing has been an issue of concern for the ACS in recent times, as evidenced by two media releases by the ACS President (ACS 2003, ACS 2004a) and the release of an ACS Policy Statement on it (ACS 2004b).

Outsourcing has also been an issue in the wider ICT industry. The Australian Institute of Computer Ethics (AiCE) has an online discussion forum. In recent months, a major focus of multiple discussion threads, has been discussions on ICT outsourcing (AiCE, 2005). AiCE membership includes ACS members and other who are associated with ICT. The latter include professionals in engineering, law, agriculture and more – all people who use ICT in the professions and want to have input into ICT matters in Australia.

Outsourcing is often defined as "the delegation of non-core operations or jobs from internal production to an external entity (such as a subcontractor) that specializes in that operation. Outsourcing is a business decision that can be made for quality or financial reasons. The term also implies transferring jobs to another country, either by hiring local subcontractors or building a facility in an area where labour is cheap." (Wikipedia, 2005). Outsourcing of jobs to another country is sometimes called off-shoring.

AiCE members saw ICT outsourcing as an issue impacting the Australian job market and ICT professionalism in this country. Members saw a number of ethical issues involved. These included the following:

Professionalism issues

- The implications on staff, such as the impact on employee control and morale. Do workers do a more professional job if they embody the firm's corporate memory or stand apart from it?
- Issues of professionalism, where corporate and individual values differ. An ICT professional has to harmonise society and corporate responsibilities. S/he professes to society that they will place society's interest foremost, in their use of their specialist knowledge.
- Issue of standardisation between the supplier and customer. This includes such considerations as the standards of professionalism such as for coding and documentation practices.
- Issues related to quality of service and the supplier's strict adherence to Service Level Agreements (SLAs). This strict adherence to an SLA may often mean that the supplier's staff are not inclined to make the extra effort for the customer, providing just the minimum of service quality.
- The issue of off-shoring and development. In developing systems, and particularly software, the hardest problem is getting a clear statement of requirements. Gathering requirements is the hardest part of software development. Requirements elicitation is a joint learning process through dynamic interactions between clients and developers, a process that involves risk of errors and misunderstandings. These inherent risks are exacerbated in outsourced and off-shored development projects, where communication is less interactive.

Privacy, copyright and intellectual property issues

- The implications on privacy and intellectual property which affect an organisation when they choose to outsource/offshore their services.
- Issues of copyright. When development occurs in-house, employers gain copyright of software written by employees. But when ICT outsourcing occurs, do contractors retain copyright of software they develop? Outsourcing contracts should address this issue clearly. Related issues are those of knowledge sharing and Intellectual Property.
- Particularly in relation to off-shoring, issues of security and privacy. Privacy laws can be different from one country to another, raising concerns that weaker privacy laws in an off-shore outsourcing situation involving work produced in another country, might affect information systems developed for the Australian context.

Social responsibility issues

- Economic ethics come into consideration too. Organisations have corporate values, for which they are responsible, for example to their shareholders. Is it ethical for a company to pay more than the most economic rate?
- Issues of casualisation and social responsibility. Casualisation involves a shift in employment from mainly full-time and permanent, or contract positions, to an increased level of casual

positions. One contributor put it this way: "Ongoing employment vs. contract: A marker of the casualisation of society [is] not necessarily an IT issue but a broader social issue and possibly a symptom of the increasing individualisation of social responsibilities."

- Issues of societal costs, such as greater unemployment in the ICT sector in Australia. Related to this is the issue of greater distribution of global wealth, increased GNP for nations to which ICT is outsourced and greater employment opportunities in those countries. Whilst outsourcing does not always lead to off-shoring, this raises issues of protectionism.

Different aspects of ICT outsourcing can be unethical, ethical or ethically neutral. Its component elements can each raise different types of ethical issues. Or they could each be seen as nothing to do with ethics, but rather as a political or industrial issue.

WHEN DO CHANGES IN ICT NECESSITATE CHANGES TO THE CODE OF ETHICS?

In a domain which changes as frequently as that of ICT, a change in work practice, or the advent of some new technology, should not of itself constitute grounds for changing a code of ethics.

Off-shoring is just one example of the type of change, which might also include the rise of the Internet or the impact of micro/nano computing; that makes us wonder about revising or reviewing our codes. Codes cannot be reviewed with every change that occurs.

To avoid ineffective continuous code reviews, procedural guidelines are needed within a professional society, that ensure regular review of its code or codes. How frequently should such a review be undertaken? Given the logistical difficulties involved, and based on observations of previous changes to codes in Australia and the USA, the authors contend that codes ought to be reviewed at least every 10 years. The ACM code was reviewed in 1992 and again in 1998, but not since. The ACS code was reviewed in 1975, and again in 1985, but not since then. By this reckoning a review of the ACS code is long overdue. The review procedure ought to also allow for reviews that are determined by major technology changes. The advent of a biological computer implanted in the brain might be the sort of thing that justifies immediate code review rather than waiting a prescribed period of time.

ICT professionals have always had to deal with the relation between ethical assessment and technology. Changes to codes of ethics have been motivated by a desire to include their expanded sense of professional responsibility and behaviour occasioned by some technological advances (Gotterbarn, 1996). Other changes were made to include an aspirational component in the code.

Why aspirational? To appeal for right behaviour, when enforcement is not possible. In medicine and law, a breach of the code of ethics can mean loss of ability to practice one's profession. Not so in ICT. An ACS member can be held accountable, through the ACS Disciplinary procedures. But 80% of ICT practitioners in Australia are not ACS members. Also, a member facing the ACS Disciplinary procedures could simply resign. Then s/he can continue to behave unethically; they simply can no longer claim to be an ICT "professional", which is a right that the Australian Council of Professions (ACP, 2005) has restricted to use by ACS members only.

Gotterbarn (2000) writing about experiences in the development of two codes of ethics in the USA found that a critical issue is that of specificity, that is how prescriptive and detailed the code should be. Specificity has partly been addressed in the ACS Code of Ethics by recent work (Bowern, 2003) which resulted in a set of case studies identifying issues related to each of the clauses in the code. Some of the cases were drawn from published material (Burmeister, 2000; and Burmeister and Weckert, 2003); others were based on actual incidents known to the authors; and a few were invented to complete the set. This exercise has revealed some shortcomings in the ACS Code. For example, the clause stating 'I must distance myself professionally from someone whose membership of the Society has been terminated because of unethical behaviour or unsatisfactory conduct' is unfair and unworkable (Bowern and Weckert, 2005).

Another approach to specificity is in the clauses of the code itself. In some instances the code of conduct does not change, but changes in ICT practice mean that the application of the code, as seen in the code of practice, is different.

LESSONS FROM THE EVOLUTION OF THE ACM/IEEE CODE

The solution to code modification is not purely technical. In the ACM/IEEE Software Engineering Code (SECEPP, 1999) it was important to include a broader sense of ethical reasoning in it. In evaluations of that Code by philosophers such as Herman Tavani, the decision making guidance of the preamble was considered one of its strengths. The international task force that developed the Software Engineering Code of Ethics and Professional Practice (SECEPP) was aware of a number of previously identified weaknesses of professional codes and made a conscious effort to address those in their code. Major motivations for writing the SECEPP was to document the professional responsibilities of software engineers, and those aspiring to be software engineers, in a way which could be used to educate practitioners and the public, and to facilitate ethical decision making in accordance with these responsibilities.

There have been two major problems in attaining these broad goals. One is based on the overly specific content of a code, in which the code attempts to define precisely a complete list of all of the ethical behaviour of a professional. Precisely defined codes are almost out of date the minute they are approved. This is especially true in professions as dynamic as ICT. On the other hand codes which are too general, which treat ethical judgement at its most abstract level, have been criticised for their failure to provide adequate guidance. This attack is often generalized into a simplistic criticism of all codes, because codes can never be complete and anticipate every possible ethical situation (Fairweather, 2001). Such criticism of codes are easily made, but are not very useful for they do not distinguish an incompleteness which is a shortcoming, from an incompleteness which is a strength. The SECEPP attempts to steer a middle ground between code imperatives which are too vague to give useful guidance, and the numbing precision of detailed imperatives which are locked to a particular stage of technology. Instead of appealing to a particular technical standard such as structured programming, which will change, the code appeals to the changing standards of the profession to address specific technical issues. By appealing to current best practices rather than naming a specific practice, as the standards change the particular technical items referred to in the code also change. This is a way to build a code which keeps current with the particular best standards of the profession.

The SECEPP code differs from that of the ACS, in that it also includes some general principles on ethical decision making to help guide the utilization of the specific clauses. For example, the preamble uses everyday English to advocate basic ethical approaches to decision making, and asks software engineers when making a decision guided by the specific principles in the code, also to:

- consider broadly who is affected by their work (utilitarianism);
- examine if they or their colleagues are treating other human beings with due respect (Kantianism);
- consider how the public, if reasonably well informed, would view their decisions (Gert and others); and
- analyse how the least empowered will be affected by their decisions (John Rawls).

The international SECEPP taskforce stated that ‘without the aspirations, the details can become legalistic and tedious; without the details the aspirations can become high sounding but empty; together the aspirations and details form a cohesive code.’ (Gotterbarn, 1999, p103)

Another concern is that in many cases it appears as if principles in a code could point in conflicting directions and thus the code itself does not direct the final decision. SECEPP admits it is incomplete, but does not suffer from issues of vagueness, because it provides general guidance for ethical decision making as indicated above. This still leaves open the possibility that the general principles may be in tension, in particular circumstances.

SECEPP has a clear hierarchy of values that facilitates the reduction of the instances of ethical tension. First its eight principles are listed in an hierarchical order. If this does not help in the final decision making, then the code has an overriding principle – that a concern for health, safety and welfare has an overriding primacy. SECEPP consists of a set of principles (code of conduct statements) and details or examples for each of the principles (code of practice statements). Its preamble contains some guidance on understanding

and using the code. It is the preamble which facilitates it addressing some of the older philosophical criticisms of professional codes.

This structure of the IEEE-CS/ACM code has raised other comments, whereby some philosophers have taken the SECEPP taskforce to task for including guidance about using the code as part of a document called a Code of Ethics and Professional Practice. As the following paragraph shows, this criticism has not deterred the adoption of the SECEPP by a significant number of software engineers.

The SECEPP taskforce identified a set of common elements to the profession of software engineering. They did this without identifying a particular professional society's preference for a particular culture's ethical style. The evidence for that is in the number of professional societies throughout the world that have adopted the Code and translated it into their native languages. Currently the Code has been adopted by professional societies in Argentina, Australia, Canada, China, Croatia, England, Italy, Israel, Japan, Mexico, Spain, and the United States.

THERE ARE CURRENTLY SEVERAL CODES FOR THE ACS

The ACS Code of Ethics (ACS Codes, 2005) comprises two sections. The first section is a simple policy statement plus a declaration of six Values and Ideals; which are then expanded into the second section, a detailed set of 37 statements, which are called the Standards of Conduct. This Code of Ethics is defined as part of the ACS National Regulations, to emphasise the importance of the code, and to ensure its prominence in the ACS body of documentation.

Supplementary to the Code of Ethics is the Code of Professional Conduct and Professional Practice (ACS Codes, 2005). This code was developed to provide more practical guidance in the day to day activities of ICT professionals. It is not part of the National Regulations, which means that it is easier to amend and update. Changes to the National Regulations require a vote by the National Council, followed by a vote by all members of the ACS. This has implications for future amendments to the codes. Figure 1 illustrates these various codes.

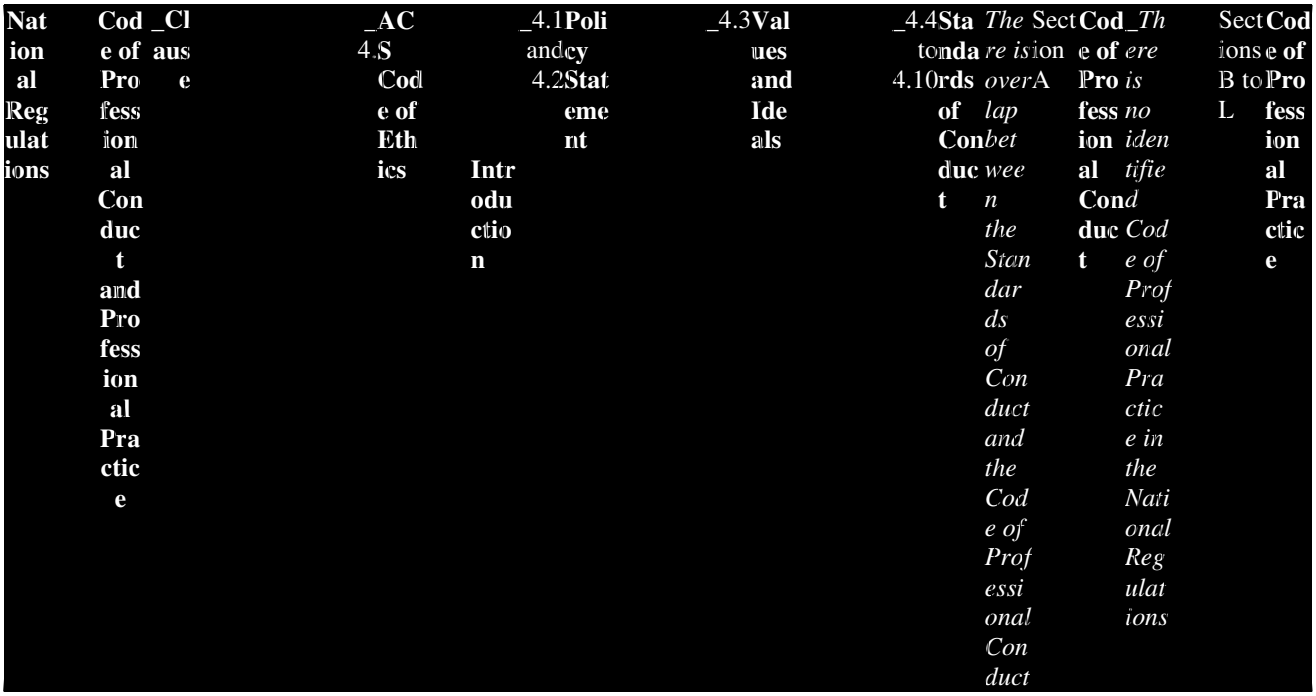


Figure 1: The "Conduct" Overlap.

The Code of Professional Conduct is 'intended as a guideline for acceptable personal conduct for each IT professional practicing in the industry', and as such it is complementary to the Values and Ideals and the Standards of Conduct. There is some overlap between these two codes of conduct.

The Code of Professional Practice is 'intended as a guideline for acceptable methods of practice within the IT industry'. The guideline is generic and addresses a range of aspects of the product life cycle, and acquisition, development, implementation and support processes. The Code of Professional Conduct and Professional Practice has never been updated since its adoption by the Society.

The ACS Code of Ethics (comprising a policy statement, the six Values and Ideals, and the Standards of Conduct) is a general code applicable to virtually anyone in the ICT industry; this is what has hitherto been referred to as the code of ethics, in this paper. There is however also the IEEE/ACM code (SECEPP) which is aimed specifically at software engineers. This second code was adopted in 2004 by both the ACS (Davidson, 2004), and the Institution of Engineers, Australia. The focus of this paper continues to be on the first, but with lessons on the development of the SECEPP code being drawn on, for recommendations of changes to the ACS code.

Future versions of the ACS Code of Ethics should:

- incorporate the Code of Professional Conduct, to ensure consistency with the Standards of Conduct, to produce a code consistent with the IFIP code of conduct;
- update and maintain the Code of Professional Practice as an equivalent to the IFIP code of practice; and
- rationalise the way that a part of the code is incorporated in the National Regulations to mandate its use, and the way that other parts of the code can be more easily updated.

In 2003 the ACS established a national Committee on Computer Ethics (CCE). Amongst its terms of reference is 'to develop and propose relevant codes of conduct' (ACS CCE, 2003, p 5). The ACS Code is in need of change (Bowern, 2003; Burmeister, 2000) because it is dated, and does not reflect ethical issues arising from technological developments, since the last major revision in 1985. Consequently it does not reflect the ethical issues of the widespread adoption of the internet, ubiquitous problems like Y2K, the human-computer interaction issues created by nanotechnology, nor does it adequately address the issues of outsourcing raised above.

The SECEPP code development has yielded lessons to be heeded. The extensive consultation process engaged in by that taskforce, needs to be emulated and followed by the ACS. IFIP also advocates an extensive consultation process, arguing that the 'process used to develop a code is as important as the code itself' (Berleur, 2004, p13).

DEFICIENCIES IN THE ACS CODE

A recent ACS report, including a small survey of ACS members active in the computer ethics field, has identified some deficiencies and potential improvements, as follows, in the ACS Code (Bowern, 2003).

- The meaning and use of the Code needs to be clarified, to explain exactly what role the Code does, and should play, as a way to provide guidance and education.
- The role and activities of the Disciplinary Committee in the ACS should be reviewed and amended, if required.
- Consideration is required of whether the Code should take into account the fact that ACS members come from different cultural backgrounds, and that they may interpret some of the clauses in different ways.
- The code should be consistent with international standards since, although the software is developed or designed in Australia, it has international consequences.
- An editing process to resolve these existing issues should be established, ensuring that the Code is maintained to reflect the changing nature of the ICT industry.

The ACS CCE have identified the following additional deficiencies:

- In 1985 the "C" of ICT was not part of the self-description of the ACS membership. The code only indirectly addresses "C" type issues at this time.
- Unlike other codes around the world, the ACS code has no system of prioritisation, for the inevitable situations of conflict between clauses in the code.
- The power of sanction (disciplinary committee) relationship to the code is poorly defined.
- The need to resolve issues to do with a multiplicity of codes of ethics. As mentioned already, in addition to the ACS Code of Ethics, the ACS has adopted the SECEPP code. Then too, there are many in the ICT industry who belong to specialist groups (management consulting, graphic design, software engineering, systems administration, human-computer interaction, and more). In some of these there are codes of ethics specific to that group. For example, the Systems Administrators Guild of Australia formed their own working group on Ethics, because they saw the ACS code as too general, lacking specificity for their work; they came up with their own code of ethics (Lance, 1994). What is the relation of the ACS code to these other codes? Should there be one single code for all ICT professionals? What about in situations like SECEPP, a second code adopted by the ACS, what happens if there is conflict between such a code and the ACS code?

Disciplinary Committee

The roles and responsibilities of the ACS Disciplinary Committee are described in the Society's Rules and Regulations. IFIP argues that 'no code has any value in terms of public duty unless it is associated with a power of sanction such as disciplinary procedures' (Berleur, 2004, p12). However, Anderson, et al (1993) have argued that codes as education serve a useful function in educating and guiding decision making.

Whilst a laudable aim, the authors contend the IFIP view is not currently achievable. Professionalism in ICT, certainly in Australia, is still not at the same level as in engineering, medicine and law. As shown above, in Australia it is possible for a member of the professional society, who has been called to account for a disciplinary matter, to simply resign their membership. Upon their resignation, no further action by the professional society can be taken. However, in other professions, such as medicine, such opting out of the society is not possible. For this reason, it is the view of the authors that the greater emphasis ought to be on 'incentive' and 'education, rather than on 'discipline', in regards to a code of ethics in ICT.

Cultural aspects

Australia has a significant multi-cultural population, which is also reflected in its ICT workforce. Certainly the Code's audience consultation process should include members who come from different cultural backgrounds.

One debate is whether the code should contain clauses reflecting the cultural differences of its members. Part of this debate is whether the clauses of the Code should have a common interpretation, or allow for contextual and cultural variances. IFIP has argued (Berleur, 2004), on the basis of Kant's 'categorical imperative', for a universalisation, in which a code contains necessary 'minimum criteria, conditions, and requirements' applicable to all members of a professional society, regardless of cultural, social and/or legal context.

The authors argue that it is not an issue of cultural debate whether testing reduces the risks of software failure. The ethical responsibilities of a practicing professional, embodied in a code of ethics, are dictated by that profession and its technology. The profession knows the best standard (its code of practice) to satisfy these responsibilities.

National aspects

Gotterbarn (1997) describes the membership of the task force for Software Engineering Ethics and Professional Practices. It comprised people predominantly from North America and Europe, with a few other members, including one from Australia. During the development of the draft codes Gotterbarn found

that North American contributions to the codes predominantly followed obligations/rights ethics, whereas the bias in Europe was towards virtue ethics. His study identified that Middle Eastern and Australian views did not easily fall into either of these categories.

To the authors of this paper, the important point is to recognise that there are different approaches to ethics and to ensure that they are considered in the development of codes for ICT ethics. These different approaches - do something because it is the right thing, or do something because it is the will of some deity, or do something because it will produce the greatest good - address the basis for a particular belief. The affirmation of intellectual property, for example, can be based on any of these approaches to ethics; but once IP is affirmed in a code it is not subject to cultural relativism. The ACM/IEEE SECEPP sought principles, consistent with each type of ethics, that were standards of software engineering.

International aspects

The ACM and IEEE are international organisations and the task force was established to recognise that international character. An objective of the task force was to establish a code which would be accepted internationally. The ACS does have international members, and has entered into reciprocal agreements with a number of overseas computer societies, including several in South East Asia. However, the ACS does not have the same sort of international ambitions as those of the ACM and IEEE. Therefore it might be argued that any redevelopment of the ACS code would generally focus on the needs and issues relating to Australian ICT professionals, although those of the international members should not be forgotten.

However, the development of computer systems and software are international activities, and have international impact; and those aspects must be reflected in codes of ethics. If the ACS is to meet the needs of the profession, it is the needs the international ICT profession that must be met. If the ACS comes up with a principle that is uniquely Australian, then we should question whether it really was a principle of the profession.

This issue of global versus Australian principles in a Code comes out in outsourcing as well. Off-shoring raises many different and interesting economic issues, but from the technical point of view as a software developer it is bad software development. In developing software the hardest problem is getting a clear statement of exactly what the customer needs and the best way to meet those needs. Gathering these requirements is actually the hardest part of software development. The elusive character of software requirements is a long-standing issue. If we characterize requirements elicitation as a joint learning process in which shared understandings evolve through dynamic interactions between clients and developers, it is apparent that this process involves risk of errors and misunderstandings. These inherent risks are exacerbated in outsourced software development projects, where communication processes are less interactive. The use of outsourcing, in any situation that mitigates against this interactive development, is inconsistent with professional software development.

Guidance and education

Further work is needed to identify how the ACS Code can best provide guidance and education to its members. Current attempts by the CCE at accomplishing this are mainly through better communication and publicity of the code to ACS members.

Some members of the CCE have produced a set of case studies related to each of the clauses in the ACS Code (ACS Cases, 2004), which have been publicised to members. Since late 2004 the CCE has arranged for a regular column in Information Age, the ACS bi-monthly magazine for members and other professionals in the industry. The column seeks to promote the code, and discuss the ethical aspects of current ICT news items or scandals. The case studies are a source of material for these articles.

The CCE will also seek to arrange regular sessions at the ACS Annual Conferences at which industry and academic speakers can address issues of the code of ethics. Already greater use of the ACS web site has been made for this purpose.

Advice should be provided on how the Code would apply to the wide range of ACS members, some of whom are not directly involved in systems development, for example ICT professionals dealing directly with customers, such as some empirical software engineers. If the ACS Code is to cater to the widest possible interpretation of 'ICT professional', it must be examined for its applicability to all aspects of the profession. An excellent example has been set through the ACM/IEEE Software Engineering Code, that has recently been adopted by the ACS for its members who are software engineers (Davidson, 2004). The adoption of the software engineering code is another contribution to the specificity of codes for the ACS.

A POSSIBLE APPROACH TO CODE REVISION

Moor (1999, p65) defines policies as 'rules of conduct ranging from formal laws to informal, implicit guidelines for action'. So a code of ethics could be considered as a set of policy statements about how a professional should behave, in ICT in this case. The on-going development of technology coupled with the malleability of computers means that there will always be a need to develop new policies.

One framework that will aid ACS deliberations is James Moor's Just Consequentialism. Moor (1999, p65) comments on the problems rising from conflicting ethical theories and believes that 'ethics needs more unifying theories that call upon the various strengths of the traditional approaches to ethics'. His Just Consequentialism theory, or framework, is discussed and summarised with respect to cybertechnology, in Tavani (2004, pp59-60). The framework consists of two steps:

- *deliberate* over various policies from an impartial point of view to determine whether they meet the criteria for being ethical policies (for example, they do not cause unnecessary harms, and support individual rights);
- *select* the best policy from the set of just policies arrived at in the deliberation stage by ranking ethical policies in terms of benefits and (justifiable) harms.

This approach would appear to be one way to consider the issues described above, and the CCE will consider its use when revising the ACS code of ethics.

CONCLUSION

Just as a motor vehicle should have regular services, so should a code of professional ethics. With a vehicle there is typically a major service infrequently, and more regular minor services. In the case of the ACS Code of Ethics, there have been numerous minor services and lots of tinkering, since the last major service in 1985. It is long overdue for its next major service.

The use of a suitable code of ethics is necessary for the successful development and implementation of new applications of ICT. It is also necessary for the promotion of public trust in the professionalism of those in ICT. Codes are a tool for assessing the ethics of new technologies, such as nanoizing technology, and new ways of working within ICT, such as the treatment of participants in a testing process, and in outsourcing services to an overseas organisation. Change in ICT is a fact of life.

Professional societies need to put in place procedural mechanisms to ensure regular (at least every 10 years) reviews of the codes, to ensure their ongoing relevance. The ACS requires ICT professionals to keep up to date with changes in the industry. No less should be required of the professional code of ethics.

How codes of ethics addressing ICT practices are changed requires deliberate thought and planning. One way is to appeal to current best practices rather than naming a specific practice, as technical standards change the particular technical items referred to in the code also change. This is a way to build a code which keeps current with the particular best standards of the profession and overcoming the risk of the code becoming out of date by rapidly changing technology.

In changing a code, there is a need to put metrics in place to ensure the efficacy of those changes. IFIP has developed high level guidelines to assess the strengths and weaknesses of a code of ethics. Such guidelines can help in this process, though more work is needed to turn these metrics into a reliable code assessment tool.

REFERENCES

ACP (2005) Australian Council of Professions, http://www.professions.com.au/ accessed on 25 July 2005.

ACS (2003) Press Release commenting on Telstra's policy on off-shoring, Australian Computer Society, http://www.acs.org.au/news/110903.htm accessed on 25 July 2005.

ACS (2004a) Press Release announcing release of Off-shoring Policy, Australian Computer Society, http://www.acs.org.au/news/020604.htm accessed on 25 July 2005.

ACS (2004b) Off-shoring Policy, Australian Computer Society, https://www.acs.org.au/acs_policies/docs/2004/OffshoringPolicy_wChecklist.pdf accessed on 25 July 2005.

ACS CCE (2003) *CCE submission to Council*, Terms of reference for the national Committee on Computer Ethics (CCE), as defined by the Community Affairs Board of the Australian Computer Society, Sydney: ACS, Nov.

ACS Cases (2004) Case Studies, Australian Computer Society, http://www.acs.org.au/publication/docs/ACS_CaseStudiesFinal.pdf accessed on 8 July 2004

ACS Codes (2005) Australian Computer Society codes, http://www.acs.org.au/ accessed on 7 July 2005.

AiCE (2005) Australian Institute of Computer Ethics, http://xindi.bf.rmit.edu.au/aice/ accessed on 6 July 2005.

Anderson, R. Johnson D, Gotterbarn D, and Perrolle, J (1993) *Using the ACM Code of Ethics in Decision Making*, Communications of the ACM, Oct.

Berleur, J., Duquenoy, P., Holvast, J., Jones, M., Kimppa, K., Sizer, R., and Whitehouse, D. (2004) *Criteria and Procedures for Developing Codes of Ethics or of Conduct*, International Federation for Information Processing, IFIP-SIG9.2.2, IFIP Framework for Ethics of Computing, Sep.

Bowern, M.E. (2003) Report to the ACS Management Committee on the ACS Code of Ethics Project, Sydney: ACS, Dec.

Bowern, M.E. and Weckert, J. (2005) *Ethics: When a team member embezzles..,* Information Age, June, viewed 7 July 2005, http://www.infoage.idg.com.au/index.php/at;1;o;7

Burmeister, O. K. (2000) *Applying the ACS Code of Ethics*, Journal of Research and Practice in Information Technology, 32(2), 107-120.

Burmeister, O.K., and Weckert, J. (2003) *Applying the new Software Engineering Code of Ethics to Usability Engineering: A Study of 4 cases*, Journal of Information, Communication & Ethics in Society, 3(3), 119-132.

Coldwell, R.A. (1987) *Non-professional Practices in Computing: Some Thoughts on the Next Decade or So*, The Australian Computer Journal, 19(4), Sydney: ACS, November, 215-218.

Davidson, P. (2004) *ACS and IEAust jointly adopt software ethics, practice code*, Information Age, Apr, viewed 24 Nov 2004, http://www.infoage.idg.com.au/index.php?id=912845172.

Fairweather, N.B. (2001) No PAPA: Why Incomplete Codes of Ethics are worse than none at all, in *Readings in CyberEthics* (eds. R.A. Spinello and H.T. Tavani), Jones and Bartlett Publishers, Sudbury, MA.

Gotterbarn, D. (1996) Establishing Standards of Professional Practice, in *The Responsible Software Engineer*, ed. Colin Meyer, Springer Verlag.

Gotterbarn, D. (1997) The Professionalization of Software Engineering and its significance for Ethics Education, IEEE, Frontiers in Education. Proceedings 1997.

Gotterbarn, D. et al. (1999) "Software Engineering Code of Ethics is Approved" in *Communications of the ACM* 42:10 102-107

Gotterbarn, D. (2000) *Two Computer-Related Codes*, Perspectives on the Professions, 19(1).

Ladd, J. (1995) The Quest for a Code of Professional Ethics: An Intellectual and Moral Confusion, in *Computers, Ethics and Social Values* (eds. D.G. Johnson and H. Nissenbaum), Prentice Hall, Englewood Cliffs NJ.

Lance, K. (1994) Crafting a Code of Ethical Conduct, SAGE-AU Code of Ethics, Systems Administrators Guild of Australia Annual Conference.

Luegenbiehl, H.C. (1983) Codes of ethics and the moral education of engineers. *Business and Professional Ethics Journal,* **2**(4), 41–61.

Moor, J. (1999) Just consequentialism and computing. *Ethics and Information Technology* **1**(1), 65–69.

SECEPP, (1999) IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice, Version 5.2.

Tavani, H.T. (2004) Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology. John Wiley and Sons, Inc, Hoboken, NJ.

Wikipedia (2005) http://en.wikipedia.org/wiki/Outsourcing accessed on 6 July 2005.

COPYRIGHT

Ethics and Systems Quality

Craig McDonald,
School of Information Sciences and Engineering,
University of Canberra, Australia.

craig.mcdonald@canberra.edu.au

Abstract

This paper links the concept of ethics with that of quality in systems development. It presents an argument that both can be effectively embedded in the systems development rather than being seen as an optional extra, external to the main task of systems development.

Keywords
Systems development, quality, ethics and responsibility.

INTRODUCTION

Producing good quality systems using good quality processes ought lead to beneficial outcomes all round and praise for the developers. Blame is deserved for systems failures resulting from carelessness, ignorance, complacency or other irresponsible attitudes.

Praise and blame are hallmarks of ethical judgments, but in systems development they are usually discussed in terms of quality, not ethics.

Perhaps explicitly building ethical principles into quality assurance is a way of both practically implementing aspects of the ACS Code of Ethics and also giving some stronger foundation to Quality Assurance. We will look at this idea by first considering Quality Assurance, then Ethics and lastly looking at a method of integrating aspects of each into the teaching of systems development.

QUALITY ASSURANCE

A 'product - process' model (Figure 1) can be used to put the idea of quality into the systems development context. This simple model identifies four aspects of development activity:

1. *Process*. The model applies at any level of process, from that used to build an entire system to some task that is a small part of the construction process. Every process

is executed in an organisational context and uses the knowledge of staff, tools and techniques, etc and may be constrained by policy, history and so on.

2. *Input - output* to and from the process. Every process has documents of some kind as input, perhaps a specification or work request. Every process produces documents of some kind as output, perhaps a manual or a code module. The output of one process is usually part of the input to another.

3. *Management.* The planning of the process, including the traditional features of the Project Management Body of Knowledge (PMI 2000, Schwalbe 2005) needed to plan, monitor and review the process.

4. *Quality.* Three points of quality assurance are identified - process quality, product quality and impact quality.

Conformance with relevant standards and good development practice is one classic means to assess quality (eg. AS/NZS ISO 9000). This method can be applied to both the process and product of systems development tasks (ISO/IEC 15288, 2000). 'Fitness for Use' is the second common quality measure. It concentrates on the relationship of the product with the actual user, that is, it views the product as tool. Early views on 'fitness for use' were expressed by the ergonomics and cybernetics communities. But there is a third, less common measure - what are the impacts of the system over and above its fitness for use? In the end, the quality of the systems we build is determined by the impacts they have on people, organisations and society.

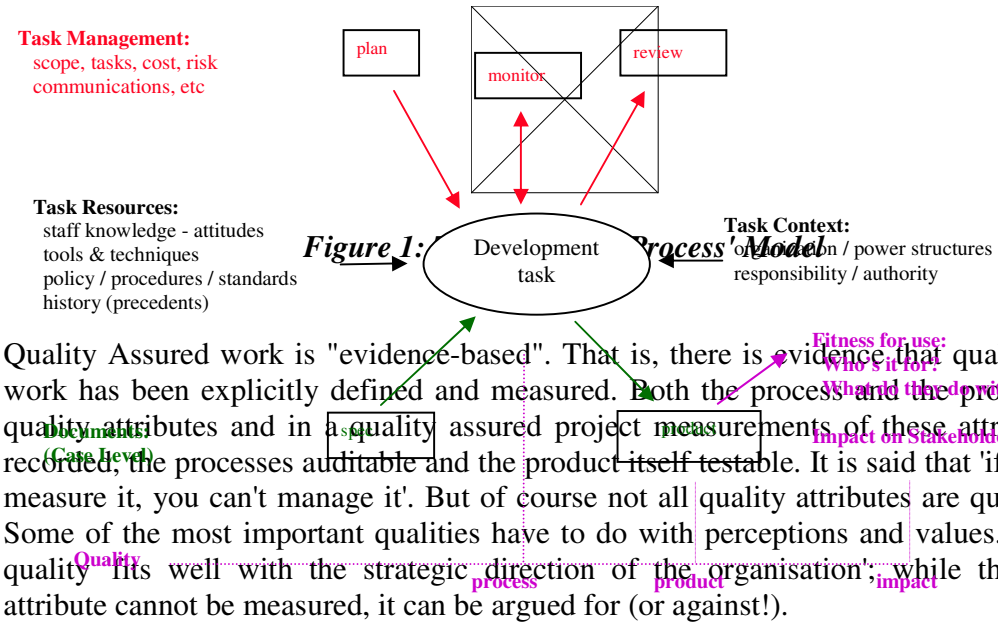


Figure 1: Process Model

Quality Assured work is "evidence-based". That is, there is evidence that quality of the work has been explicitly defined and measured. Both the process and the product have quality attributes and in a quality assured project measurements of these attributes are recorded, the processes auditable and the product itself testable. It is said that 'if you can't measure it, you can't manage it'. But of course not all quality attributes are quantitative. Some of the most important qualities have to do with perceptions and values. Take the quality 'fits well with the strategic direction of the organisation'; while this quality attribute cannot be measured, it can be argued for (or against!).

While there are general quality standards, 'quality' always relates to some specific object, event or impact. General ideas about what to measure (correctness, modifiability,

testability, usability, reliability, efficiency, integrity, reusability, interoperability, etc.) can be useful guides but each unique product, process and impact needs its own quality criteria to be established and satisfied.

This proposition leads to the idea that every single product and process needs to have embedded in it the means to assess its own quality. Imagine for instance each object in an object-oriented system having not only its own data and services, but also its own methods of evaluating itself.

We return to quality shortly.

ETHICS

There seems to be three main kinds of discussion about ethics and ICT. The first tackles particular issues, like workplace surveillance or copying software, and examines the ethical principles that might apply to them. Laws are framed from this kind of discussion so it is critically important.

The second kind of discussion looks at specific events, real or made-up. Particular situations throw up unusual ethical aspects and dilemmas that highlight the complexities of ethics. For example, the set of ACS ethics cases reveal the complexities and contradictions that are inherent in ethical considerations of the particular situations we all find ourselves in sometimes (http://www.acs.org.au and search for 'code').

The final kind of ethical discussion starts from first principles and sees issues and events as applications of ethical principle. For example, if the principle of 'the greatest good for the greatest number' were to be applied to a situation, how would we measure 'good', can we add it, how could we balance the good to one person against that to another, etc. Despite such problems, the first principles approach that has given us a valuable practical tool for ethical evaluation - stakeholder analysis.

There are different kinds of stakeholders (Pouloudi 2000). Those that can terminate the project (financiers and clients) are most obvious. The stake they hold has sometimes been likened to a garden stake - sharp ended and potentially lethal! The next stakeholder is like a gambler who is part of the game, who knows the rules and whose stake is a pile of chips to bet with. Unions, insurance companies, regulators and so on are in this category. Then there are the victims; they are the ones who are impacted by systems in which they have no say. And lastly the voiceless stakeholders - the society at large, the economy and the environment (Bowern et.al. 2004)

So, it seems that the affects of our systems on our stakeholders is a core idea behind both Ethics and Quality. Systems developers are at the sharp end of these issues because their work has significant and wide-spread impacts on others. It is an ethical as well as a quality stance to care about the affects of our actions and to take responsibility for them.

Of course there are limits to what we can be responsible for. Bittner & Hornecker (2002) argue that to have responsibility for an action (or not taking an action) in some situation, a person needs to have an element of voluntariness, autonomy, foresight and there needs to be a causal influence between the action and the effect. Complex organisations & large systems diffuse and disguise responsibility. It is difficult for one person to take responsibility as effects emerge from a mix of actions and interactions that can't be attributed to a single person. Also technology and the division of labour in systems developments means that responsibility for certain components may be clear, but liability for the whole is less clear.

Nonetheless, if each of us embedded the responsibility idea into our actions the overall quality of systems would improve.

EMBEDDING ETHICS AND QUALITY IN SYSTEMS DEVELOMENT

One way to embed both quality and ethics into our systems is to explicitly cater for exactly who will be impacted by the process we are involved in and the product we will deliver.

At the University of Canberra we are trying to embed this recognition in our computing education by having students specify quality criteria for each development process and deliverable they engage with. PMSS is a computer system used to support our systems development and project management units. It has the usual facilities for planning and monitoring development, tracking issues and risks, organising meetings and for communication and configuration management.

PMSS also contains a set of templates for typical project documents. Figure 2 shows the deliverables page of our Project Management Support System. Notice that these templates are organised by stakeholder type. The interests and responsibilities of these stakeholders are the key to developers doing work that is both good quality and ethical.

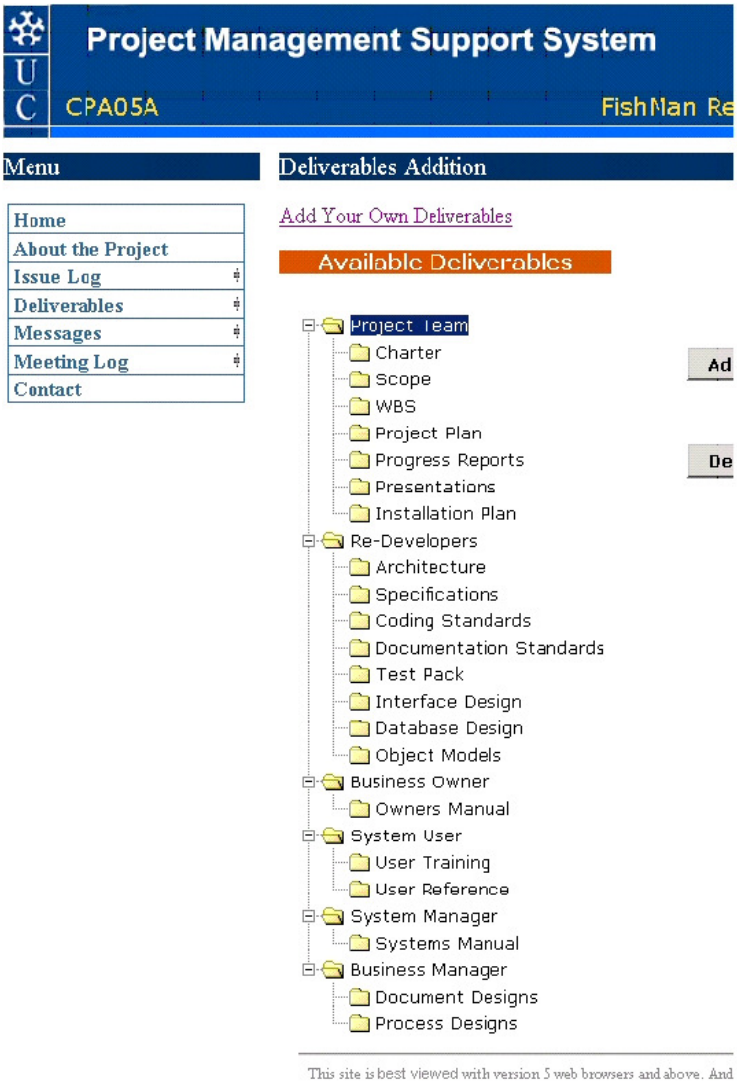


Figure 2: Deliverables page of the Project Management Support System

At the start of a project, typical stakeholders include the following a) The project team itself, which is responsible for the professional conduct of the project and for meeting the needs of the team members; b) The re-developers, those who have to understand and change the system in the future; c) The system/business owner, who as an investor expects to benefit from the returns the system brings; d) The system's immediate users,

who interact directly with the system and who have to adapt to the changes it brings; e) The systems manager responsible for the operations of the technology including security, backups, etc; f) The business manager, who administers the departments in which the system has been implemented.

Of course, as each project is unique, the range of stakeholders diverges rapidly from the typical case. But if the principle of catering to all stakeholders is sound, then lessons learned from typical cases can be applied to each new situation.

To implement quality assurance in the PMSS, each template has a set of quality criteria built in as the final section of the document. The idea is that every process and every product should have its specific quality criteria made explicit. Figure 3 shows an example of this section from a System's Owners Manual.

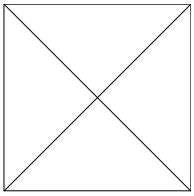


Figure 3: Quality Assurance Section of a System Owner's Manual

The System Owner's Manual may be created for upper management level executive responsible for the business area in which the system is installed. The opportunity to design executive level facilities into operational systems is often neglected in favour of more mundane data processing aspects. The very existence of this template in the PMSS raises the awareness of the student developer that she has to actually consider the executive level in the environment that surrounds her technical designs. Similarly, system's technical manager, as a stakeholder, needs diagnostic facilities built into the system in order to be equipped to carry out their task.

Once the student developer recognises that each stakeholder deserves explicit individual consideration, the scene is set for responsible and quality design work.

The assessment of student's work reinforces the idea of embedding ethics and quality into their systems development work. The assessment is conducted this way:

1. Product and Impact quality is examined from the standpoint of each stakeholder including:
   system owner - how do I know I am getting the benefits promised?
   various operational users - can I use this system?
   line manager - can I better manage the workflow of this business process?
   external stakeholder - am I being affected, perhaps by doing work that used to be done
   internally, or carrying risk?
   next developer - can I modify the system easily
   systems manager - can I ensure the stability, reliability, resiliance of the system?
   auditor - can I examine the system ?
   The academic is in the role of auditor in the assessment of the project.

2. Process quality is examined using the evidence collected in PMSS of project planning, modification and review; team management; communication, information & configuration management; and risk prevention, detection, and correction.

3. Student's individual reflection and their assessment of the contribution of their peers is coupled with reviews from clients and other stakeholders. Finally, the tutor’s review focuses on the innovation and creativity students bring to the task, their

perception and insights and the way they have built their own learning and development into the process of system development.

The PMSS is set in an educational context. But it points a way forward to a practical embedding of ethics within the quality framework of systems development. And it gives a grounding for why quality assurance can be much more that a management overhead in systems development.

CONCLUSION

Quality and Ethics go hand in hand. Every time we question the quality or ethics of a process or product we improve the system of which it is a part and we improve our own personal capability to do the right thing. These improvements are not trivial.

Being responsible for your action (or inaction) involves knowing who will be affected by your action, knowing the affects, caring about them then acting. A responsible person is prepared to accept the praise or blame.

This paper links ethics with quality then presented an argument that both can be effectively embedded in the systems development rather than being seen as an optional extra, external to the main game.

REFERENCES

AS/NZS ISO 9000 (2000) Australian/New Zealand Standard AS/NZS ISO 9000:2000 *Quality management systems-Fundamentals and vocabulary.*

Baskerville R., Stage J., and DeGross J.I ed. (2000) *Organizational and Social Perspectives on Information Technology* Kluwer Academic Publishers, Boston.

Bittner P. and Hornecker E. (2002) *Responsibility and the Work of IT-Professionals* http://www.media.tuwien.ac.at/e.hornecker/Papers/hcc6-ehpb_publ.pdf (accessed August 2005)

Bowern M., McDonald C. and Weckert J. (2004) "Stakeholder theory in practice: Building better software systems" *Proceedings of Ethicomp 2004*, Athens, Greece.

ISO/IEC 15288 (2000), *Life Cycle Management – System Life Cycle Processes, Committee Draft 2, 21 January 2000.*

PMI (2000) *A Guide to the Project Management Body of Knowledge-2000 Edition*, excerpts at http://www.pmi.org/info/PP_PMBOK2000Excerpts.asp (accessed August 2005)

Pouloudi A. and Whitley E.A. (2000) "Representing human and non-human stakeholders: on speaking with authority" in Baskerville et al. pp 340-354.

Schwalbe, K (2005) *Information Technology Project Management* 4th.ed.Thompson Learning.

COPYRIGHT

Global Software Development: The Ethical Challenge of Requirements Elicitation

Merete Crofts
School of Information Systems
Deakin University, Victoria, AUSTRALIA
merete.crofts@deakin.edu.au

Shona Leitch
School of Information Systems
Deakin University, Victoria, AUSTRALIA
shona@deakin.edu.au

Abstract

Requirements Engineering is facing an emerging set of challenges, which is compounded by traditional challenges that have always faced this area of Information Systems (stakeholder identification, domain expertise, communication, analytic skills, problem solving.) In particular the world of global software development, that has requirements teams working in virtual mode (possibly on different continents), with the software having to operate in multiple contexts, addressing the needs of different cultures and legal jurisdictions, and having to build sales in different marketplaces. This makes the challenge of eliciting requirements potentially ethically challenging and complex.

1. Introduction

Requirements Engineering (RE) has emerged over the last twenty or more years, as a discipline focussed on both understanding and producing tangible improvements to the processes, techniques and tools employed when eliciting, representing and validating user needs for systems to support various organisational objectives (where the concept of organisation is used to represent any collection of purposeful activities). Much has been achieved, with substantial advances in understanding areas such as stakeholder identification, required domain expertise, communication, analytic and problem solving skills etc., although arguably these have still not been fully addressed.

In this paper we argue that there has been, over the last several years, an important shift in the organisational context facing the requirements engineer. This is the challenge of RE in the world of global software development, with requirements teams working in virtual mode (possibly on different continents), with software having to operate in multiple contexts, addressing the needs of different cultures and legal jurisdictions, and having to build sales in different marketplaces. Further the need arises to make sure that the requirements elicitation process is trusted by members of remote teams.

To start this discussion we present a selection of theoretical models, taken from various possible source disciplines, which may offer insight into some aspects of RE in support of global software

2. Motivation

Information systems developments are notoriously difficult. The ultimate test of a delivered system is arguably how well it represents the stakeholder's needs and whether it is developed on time and within budget [1]. Failure records show that over 30% of projects are cancelled before they are completed [2] and 40% of software developments are never used after completion [3]. Statistics also indicate that on average only 16% of software projects are delivered on time and within budget, and this percentage is substantially less for developments for large organisations [2].

In view of the cost to industry of such failures to meet target, much research has been undertaken to address issues involving the balancing of features, cost constraints and schedule deadlines [4]. The focus of research needs to shift to the elicitation processes and to stakeholders in the areas of stakeholder identification, domain expertise [4] and communication skills [5] on the client side of the project and also questions of the analytical, problem-solving [6] and the communication skills of the engineers on the development side.

n particular, global software development must not only address the complexity of client and engineering teams communicating, but also the complication of lack of face-to-face discussion [7], time-zone problems [8], knowledge management issues [9] and cultural differences [10]. Further, analysts are faced with generating not just a single model relevant to a proposed system but rather a model that retains the most desirable system features consistent with the client's budget and timeline [4]. This preferred model emerges from negotiations, judgements and perceptions involving developers, marketers, and financial directors [11].

Requirements elicitation research has focussed on methods such as facilitated group sessions and workshops, brainstorming, interviews and observations [1]. Although some important models have emerged [9], research into global software development, where stakeholders and developers are typically several steps removed from each other, is still in its infancy. There are few if any workable models and associated theories to help the understanding of the special issues surrounding teams working in this virtual mode.

Contemporary organisations frequently work across international boundaries, with distributed analysis teams collaborating on global releases of software; software that might have a common core but often has special features that are unique to local laws and customs. To build our understanding of the issues, we need to examine how software development teams build and share mental models of problem domains and possible solutions, in particular when working in distributed or virtual environments.

There is some emerging evidence that training in perceptual skills greatly improves decision-making processes [12]. However, much of the research into mental model sharing has been conducted in academic situations or laboratory environments. The relevance of behaviours observed in experimental studies, to those of industrial professionals, is questionable. Several authors have questioned a lack of industry based research in the area of global software development [13].

To progress our understanding of the problems faced by requirements engineers working in the world of global software development, we suggest that two principles should underpin future work:

1. Researchers must be prepared to draw upon a range of theory sources, drawn from a selection of source disciplines such as team and project management, human learning and knowledge creation, development and sharing of mental models, and associated psychology theories and cultural and sociological understandings; and
2. Researchers must move beyond laboratory settings, and observe and analyse the behaviour of such teams in situ (i.e. in industry).

By undertaking these tasks developers can promote a better requirements process and provide a safe, open workspace for individuals. With a clash of cultures, experiences and customs it is important for a global software developer to have an ethical understanding of the difficulties that these teams may face**.**

3. Requirements engineering

Requirements engineers determine the specification of a system. At the specification stage the development team builds an understanding of stakeholder needs, following an iterative process of eliciting, analysing, representing, documenting and validating information [14]. These activities require the analyst, on one hand, to have personal skills in the form of both formal and practical knowledge [15] and on the other, to have interpersonal skills to identify users and other stakeholders, understand their problems or needs and finally to specify a satisfactory system from the obtained material The dialog between the analyst and stakeholder does not reflect the participants' views but rather helps to develop a concept of perceived reality or mental models of the issues . Systems development is therefore an iterative never-ending learning system very much based on the analyst's and stakeholder's judgements and communication abilities [16].

The most crucial aspect of information systems development is gathering and validating the requirements. This is difficult because requirements come from both technical and social domains. The technical element is fairly straight forward to identify, but how do you capture and validate the requirements of a social domain where values and decision making is embedded in a unique organisational culture [6]. Blyth identifies that the best source of requirements is domain knowledge and that the stakeholders are the holders of domain knowledge. Many of the reported difficulties in requirements analysis are associated with linking problem owners and problem solvers [1]. The initial issue for analysts is therefore to identify the appropriate stakeholders and other parties that may be affected by the proposed developments. Without the support of key decision-makers to approve the developments on one hand and concerned individuals on the other, successful solutions and implementations are in serious doubt. Analysts must also address questions of why and how some information flows are important and meaningful and why a goal is important and from where it originates [6].

Vickers explains that systems analysis should not be seen as a method for solving problems but rather as a means of understanding situations. By doing this the creation of a more complete and user driven ethical system can be achieved. Once a situation is fully understood, both what can and what needs to be done can become apparent [8]. Systems

development rests on analysts' and stakeholders' judgements and communication abilities [16].

3.1 Team thinking

Projects and tasks of significant size are assigned to teams or business consultants because of time and knowledge constraints. The amount of work in the allotted time is greater than one person can possibly achieve and the required knowledge and skills are more than an individual possesses. Further, a wide breadth of knowledge is able to produce higher standards and quality [17].

Each individual analyst will hold their own mental model underpinning their understanding of the required system which, during the course of investigation will be synthesised with the mental models of other development team members and stakeholders, progressing to a unified specification/ design. This process requires that their conceptualisations of both problems and solutions must be, in some sense, compatible [18]. Mental models are able to describe the purpose and form of systems and to explain the functions and states of what the system is doing. Furthermore, analysts are able to *run* mental models to predict outcomes and future states of a system [19]. These are important mechanisms that underpin the requirements engineering processes.

Over the years, investigation into individual mental model construction has been patchy, at best. The behaviourist movement argues that psychology is a purely objective and experimental branch of natural science, 'the science of behaviour'. Methodologies available to relate emotions or motives however, even for well trained subjects, are of questionable adequacy. It is generally agreed that research based on linguistic material is far more controllable than empirical research on mental imagery [20]. For example, some interesting investigations have been completed into the functions of an air-line crew and pilots, both in flight simulations [21] and in real-time air disasters [12]. And there are now further developments in techniques, methods and the analysis of team mental models which enable more rigorous research into shared mental models [22].

Organisations usually employ teams to increase productivity; however, some say that this increase in cognitive power can lead to a whole that is less than the sum of its parts. Sources of failure in team production include poor communication, inadequate situation assessment and pressures to conform [23]. Walz has found that there are two states where individuals may hamper coalescence of a design. Firstly, if their mental models or goals are too different or incompatible and secondly, if team members have incomplete mental models due to lack of knowledge in the relevant area [18]. Group software design is usually highly complex and time driven and therefore requires exceptional cooperation and communication between the members.

3.2 Working globally

Studies into global teams focus on the problems of communication across space and time [8], on trust [24] and on culture differences. Global teams use a variety of tools and technologies such as phone, video conferencing, email and groupware [25]. On one hand, the literature argues that working across time zones creates time management problems. A situation, such as waiting for the response to an email becomes very frustrating when

taking weekend closure into consideration [25]. On the other hand, some studies have found that teams are able to utilise time differences and technology to hand over development at the end of the working day to the team where the day has just begun, creating round the clock productivity [8].

Research into the issue of trust describes it in the context of knowledge sharing. Strong ties between employees appear to facilitate knowledge sharing, the link being trust. Trust is of two specific types: benevolence-based; and competence-based. Benevolence-based trust is built on the notion that one person will not intentionally harm the other. Opportunistic or egotistic behaviour, such as manipulation of organisational politics and competitive pursuits of career opportunities, might be considered as abuses of benevolence-based trust [26]. Competence-based trust is important to knowledge sharing because we need to believe that the other person brings adequate and reliable skills and knowledge to a relationship. This is particularly important when working across space and time. Jarvenpaa found that a high level of trust was important to productivity and morale in virtual teams. Her research suggests that some transient teams develop *swift* trust as a mechanism to enable the members to work more efficiently from the start. There is no time to examine and develop the individuals' feelings and commitment, so team members chose to take skills and dedication for granted [27]. Such teams appear to enjoy high levels of positive feedback and knowledge sharing [24].

Research into the problems of transferring knowledge has discovered that the sharing of simple knowledge in teams that are dispersed and have infrequent interaction (*weak ties*) is more efficient than in closely related knowledge workers with *strong ties*. It is therefore thought that effective knowledge sharing depends more on trust than on the links between know- ledge workers. It has also been found that knowledge sharing is reciprocal and that valuable global professional networks are formed exercising this practice [28].

Culture might be defined in terms of the degree of shared values and beliefs that the members of a community have in common. It is clear that global cultural differences will influence decision making, knowledge sharing and communication in general but organisational culture is also important. Organisations are intrinsically different; two organisations operating in the same business environment will not necessarily deliver the same end product. Groups of people create a unique set of meanings that are transmitted to new and existing members and enforced by the interactions in performing the daily tasks. These interactions create, modify or sustain the organisational culture. Therefore, some parts of organisational learning are bound to a specific organisation. It is possible to imitate other organisations but it is the collective knowledge that makes the outcome distinctive [29]. Organisational culture influences knowledge creation, distribution and storage in ways that should be identified when examining knowledge related behaviours.

Organisations may have explicit corporate culture and politics, often stated by management through the mission statement and other articulated means. However, the implicit subculture and the hidden assumptions that underpin it, are a great influence on what is perceived as relevant knowledge [30]. Management may, for example promote one type of knowledge sharing behaviour as being desirable but actually reward another by means of promotions [31]. Moreover, people are often not aware that they hold knowledge that is either unique or crucial; it remains tacit but can be conveyed through socialising.

Much of this research is done in academic environments comparing face-to-face communication with technology based situations [32]. However, it is possible to draw a sensible connection between similar themes from the literature that describes global teams working on different product development. For example, useful research has been done on experts working as virtual teams, both in developing solutions to a complex rocket design and also in developing industry technology solutions in general. These studies focused on technology and structure adaptation and extended adaptive structuration theory [32]

3.3 Knowledge sharing

The requirements elicitation stage might be considered as a learning and knowledge sharing process. The notion of knowledge sharing and knowledge management has created a great deal of interest during the last decade. Much has been written about the definitions of knowledge types and levels to facilitate knowledge creation, storage and dissemination. Research into organisational behaviour and knowledge management is thought to be important to explain knowledge sharing in team situations.

De Long and Fahey have identified three types of knowledge and explained the tacit degree in each: human knowledge that is manifested in skill and expertise and is both tacit and explicit in nature; social knowledge that exists only in relationships between individuals such as colleagues and social networks and is largely tacit knowledge; and structured knowledge which is embedded in rules, processes and organisational systems and obviously explicitly enforced. Levels of knowledge can be viewed as the process of learning that becomes a person's knowledge, which is then stored as memory and is a reflection of personal wisdom.

Much research is focused on the capacity and limits of the human mind and most researchers agree that learning involves a shift in the mind [33]. A learner's stored understandings and experiences are altered or created and recreated in a continuous process. Learning is therefore about making *meaning* out of experiences as they present themselves. Many authors subscribe to the notion of learning from mistakes and that individual and organisational learning can be observed if some change has taken place. In this theory, organisational learning is tied to an increase in performance; we behave more efficiently if we have learned

Researchers agree on one hand to the cognitive perspective of organisational learning but on the other also recognise that individual learning in organisations relies very much on social interactions and human relationships. Fiol has pointed out that organisational learning is not embedded in any single person but instead entails the ability to share a common understanding. *"Collective learning, by definition, encompasses both divergence and convergence of meaning that people assign to their surrounding"* [34].

It is generally agreed that knowledge is needed to make informed decisions [35] but residual organisational memory embedded in culture, values, structures and systems can make it difficult for organisations to learn and implement new ventures. The memory of past failures cannot simply be unlearned, especially the cognitive maps that connect

organisational outcomes and actions [34]. However, Klein (1986) has found that employees will resist learning that is imposed rather than gained through experience and will return to *tried and true* methods rather than follow the new instruction [36].

A major barrier to knowledge sharing lies within an organisation's political system - namely interest, conflict and power. An employee's interest is divided between the job or task, career and ambitions and personal life. Conflicts often arise when interests are unbalanced. Organisations openly promote competitive environments between peers to extract that *extra mile* from employees. Such rivalry can be pitted against teams, divisions and other organisations. The importance of power is increasingly being recognised as a powerful force of control. It guides how, when and to whom information is distributed. The controllers can hoard crucial knowledge so they are perceived by the organisation as either expert or indispensable. This may enhance the individual's promotional possibilities but it is detrimental to the success of Knowledge Management systems [37]. The policies of an organisation are therefore responsible for why some organisations actively learn from their mistakes while others foster an environment where errors are covered up [31]. This is supported by the theory that closely related teams can develop a culture of recycling redundant information whereas knowledge workers with *weak ties* are able to provide access to unique and new ways to solve problems [38].

A knowledge-sharing environment is not necessarily part of a globally connected community. Successful knowledge transfer appears to be closely related to trust and developments of relationships rather than proximity. However, in complex knowledge transfers and knowledge creation, face-to-face encounters are still considered essential [39].

In Table 1 (next page), we collect the various elements of theory uncovered in the review of literature drawn from the four domains discussed previously, and group them according to various viewpoints that might be taken in future research into assisting understanding and improving developers understanding of groups in the RE and global software development process.

4. Theories

4.1 Group 1: Theories of organisational behaviour

"Theories of organisational behaviour", focuses on how individuals view themselves, and how they form coalitions within the organisations to which they belong.

According to social identity theory, people have a perception of how they fit into various social categories, such as gender, age, nationality, and organisational membership. People use this categorisation process, both to identify others and to define their own position in a social environment [40]. Social identification may therefore be a useful framework to support building an understanding of the individual and team behaviours that may or may not appear rational to an outsider. Social identity is likely to affect group values, practices and prestige and the influence of competition within and between groups and is therefore also expected to impact the communication and decision making processes of requirements teams [41]. Although to a developer the categorising of social identity may well be relevant, care must be taken not to alienate team members. It is ethically unsound to categorise individuals in detail and therefore make assumptions

as to their possible decision and behavioural processes. It is a very fine line that the developer must tread in order to achieve a functioning team by understanding differences without making those differences divisive.

4.2 Group 2: Source disciplines of requirements elicitation

"Source disciplines of requirements elicitation", focuses on how individuals share data, ascribe meaning to that data, and solve problems.

Consistent with Vickers' concept of an appreciative system, it is expected that the communication and problem solving attitudes of a team will be influenced by individual and collective perceived values and beliefs. Vickers explains that reality is perceived selectively and valued judgements are made of the elements in the communication process, depending on life experiences [5].

Body of Literature	Model or Theory	Area of Application	Group 1 Theories of Organisational Behaviour	Culture Power Politics	• Identity theory • Faction alism & Coalition Formation models	Affects both individual's satisfaction and effectiveness – deals with issues of cultural identity Focusing on how resources and power distribution affect coalition formation	Group 2 Source Discipline s of Requirements Elicitation	Judgement & Perception	• Viewers' Conception of an Appreciative System	Reality is perceived selectively and value judgements are made of elements in the communication process depending on our life experiences	Problem Solving	• The Goal Seeking Model • The Relationship Maintenance Model	How do people make decisions? What are the motivations underpinning decisions?	Learning Knowledge Memory	• Organisational Knowledge requirements • Knowledge Categories and Transformation Process • Knowledge sharing	Different knowledge type Creation mechanisms for communicating.	Mental Models	Defining Mental Models, Purposes of Mental Models • Shared Mental Models	Explains the functions of mental models. Explains the evolutionary steps in the requirements specification process May provide an explanation of team performance	Group 3 Theories Pertaining to Virtual Teams	Group development	• Developmental Sequence in Small Groups	The stages of group development may explain behaviour and interactions	Time, people, purpose and links. Information sharing	• Periodic Table of Organisational Eley – ments • Information Sharing • Transactive Memory • Group Learning • Cognitive Consensus	Ability to view several points of view simultaneously – how teams move in time A practical way of categorising observed elements in a two-dimensional space	Trust	• Swift Trust • Benevolent & Competence–based trust	Trust is believed to be an important factor in effective communication & knowledge sharing	Interaction	• Distributed Cognition	Understanding human-computer interaction

Table 1: A classification of theoretical elements potentially relevant to RE

4.3 Group 3: Theories pertaining to virtual teams

"Theories pertaining to virtual teams", focuses on issues of team development and structure when members are distributed, relying upon electronic communication technologies.

Various types of trust have been identified in the literature, including *swift*, *benevolent* and *competence* based trust. Swift trust is potentially important to understanding transient teams given that teams (in Global Software Development) have neither the time nor opportunity to develop benevolent or competence trust in face-to-face meetings.

Information sharing and interaction refers to information already held by team members before discussion begins. It is included here because theory in this area argues that shared information is more likely to enter discussion than new information [42]. In principle, teams produce better decisions by pooling knowledge; however distributed cognition theory suggests that teams promote a rehashing of shared information at the expense of unshared information. Transactive memory is a social relationship phenomenon where people often supplement their own unreliable memory by engaging other people's opinion, usually experts. This suggests both a convergence of knowledge and the notion of dividing work loads, for example. Further it is expected that group learning theories [43] and cognitive consensus [44] may be able to assist with the understanding of how global teams share knowledge and define and conceptualise key issues.

5. Conclusion

In this paper we have argued that Requirements Engineers and developers face an emerging set of challenges, which compound the traditional RE challenges (stakeholder identification, domain expertise, communication, analytic skills, problem solving, ...) that have arguably still not been fully addressed. This is the challenge of RE in the world of global software development, with requirements teams working in virtual mode (possibly on different continents), with the software having to operate in multiple contexts, addressing the needs of different cultures and legal jurisdictions, and having to build sales in different marketplaces. This poses a unique set of challenges for developers including the social and ethical considerations of requirements elicitation.

We have examined the motivation for this emerging stream of RE research, that relevant ideas might be drawn from a number of associated source disciplines. A selection of such possible theory elements has been presented. The intention is to introduce the situation at a case study site, which is to be the focus of a substantial future research stream looking at the ethical and practical issues and considerations that are important in the requirement elicitation process in Global Software Development.

REFERENCES

[1]. Gause, D. and G. Weinberg, *Exploring Requirements: Quality Before Design*. 1989, New York: Dorset House Publishing Co. Inc. 299.
[2]. The Standish Group International, I., *The Chaos Report*. 1995. p. 9.
[3]. Davis, A.M., *The Requirements Triage: Deciding What to Build*, D. University, Editor. 2004: Melbourne.
[4]. Davis, A.M., *The Art of Requirements Triage.* IEEE Computer Society, 2003. **March**: p. 42-49.
[5]. Vickers, G., *Human Systems are Different*. 1983: Harper and Row.
[6]. Vickers, G., *The Poverty of Problem Solving.* Journal of Applied Systems Analysis, 1981. **8**: p. 15-21.
[7]. Warkentin, M.E., *Virtual Teams Versus Face-to-Face teams: An Exploratory Study of a Web-Based Conference System.* Decision Sciences, 1997. **28**(4): p. 975-996.
[8]. Gersick, C.J.G., *Time and Transaction in Work Teams: Toward a New Model of Group Development.* Academy of Management Journal, 1988. **31**(1): p. 9-41.
[9]. Damian, D. and D. Zowghi, *The Impact of Stakeholders' Geographical Distribution on Managing Requirements in a Multi-site Organization*. 2002, University of Technology, Department of Software Engineering: Sydney. p. 11.
[10]. Hofstede, G.H., *Cultures and Organizations: Software of the Mind*. 1997, New York: McGraw-Hill. 279.
[11]. Shaw, M.L. and W.J. Brian, *Modeling Expert Knowledge*, in *Readings in Knowledge Acquisition and Learning: Automating the Construction and Improvement of Expert Systems*, B.G. Buchanan and D.C. Wilkins, Editors. 1993, Morgan Kaufmann Publishers: San Mateo, California.
[12]. Orasanu, J.M. *Shared Mental Models and Crew Decision Making*. in *Twelfth Annual Conference of the Cognitive Science Society*. 1990. Cambridge, MA.
[13]. Sole, D. and A. Edmonson, *Bridging the Knowledge Gaps: Learning in Geographically Dispersed Cross-Functional Development Teams*, in *Strategic Management of Intellectual Capital and Organizational Knowledge*, N.B.C.W. Choo, Editor. 2000, Oxford University Press.
[14]. Herlea, D.E., et al., *A Compositional Knowledge Level Processing Model of Requirements Engineering.* International Journal of Software Engineering and Knowledge Engineering, 2002. **12**(1): p. 41-75.
[15]. Crofts, M. and P. Swatman. *Investigating Information Systems Analysts' Possession of Tacit Organisational Knowledge*. in *HICSS-35*. 2002. Hawaii: IEEE.
[16]. Checkland, P., *Systems Thinking, Systems Practice*. 1999, West Sussex: John Wiley & Sons, Ltd.
[17]. Shaw, M.E., *Group Dynamics: The Psychology of Small Group Behavior*. 3rd ed. 1981, New York: McGraw-Hill.
[18]. Walz, D.B., *A Longitudinal Study of the Group Design Process*. 1988, The University of Texas at Austin: Austin. p. 195.
[19]. Williams, M.D., J.D. Holland, and A.L. Stevens, *Human Reasoning About a Simple Physical System*, in *Mental Models*, D. Gentner and A.L. Stevens, Editors. 1983, Lawrence Erlbaum Associates, Publishers: New Jersey.

[20]. Paivio, A., *Imagery and Verbal Processes*. 1971, New York: Holt, Rinehart and Winston, Inc. 595.
[21]. Thordsen, M.L. and G.A. Klein. *Cognitive Processes of the Team Mind*. in *International Conference on Systems, Man, and Cybernetics*. 1989.
[22]. Langan-Fox, J., S. Code, and K. Langfield-Smith, *Team Mental Models: Techniques, Methods and Analytic Approaches.* Human Factors, 2000. **42**(2): p. 1-30.
[23]. Orasanu, J. and E. Salas, *Team Decision Making in Complex Environments*, in *Decision Making in Action: Models and Methods*, G.A. Klein, et al., Editors. 1993, Ablex Publishing Corporation: Norwood, New Jersey. p. 480.
[24]. Jarvenpaa, S., K. Knoll, and D. Leidner, *Is anybody out there? Antecedents of Trust in Global Virtual Teams.* Journal of Management Information Systems, 1998. **14**(4): p. 29-64.
[25]. Carmel, E., *Global Software Teams*. 1999: Prentice Hall.
[26]. Eggert, A., *The Role of Communication in Virtual Teams.* Electronic Journal of Organizational Virtualness, 2001. **3**(2): p. 1-7.
[27]. Markus, M.L., *Electronic Mail as the Medium of Managerial Choice.* Organisation Science, 1994. **5**(4): p. 502-527.
[28]. Dixon, N., *Common Knowledge: How Companies Thrive by Sharing What They Know*. 2000: President and Fellows of Harvard Collage. 188.
[29]. Cook, S. and D. Yanow, *Culture and Organizational Learning.* Journal of Management Inquiry, 2001. **2**(4): p. 373-390.
[30]. Schneider, B., *Organisational Climate and Culture*. Frontiers of Industrial and Organizational Psychology, ed. I. Goldstein. 1990, San Francisco,: Jossey-Bass Inc. 449.
[31]. Argyris, C., *Overcoming Organisational Defenses: Facilitating Organisational Learning*, ed. J. Peters. 1990, Boston: Allyn and Bacon. 169
[32]. Majchrazak, A., et al., *Technology Adaptation: The Case of a Computer-Supported Inter-Organizational Virtual Team.* MIS Quarterly, 2000. **24**(4): p. 569-600.
[33]. Senge, P., *The Fifth Discipline: The Art and Practice of the Learning Organization*. 1990, Sydney: Random House Australia Pty Ltd. 424.
[34]. Fiol, C.M., *Consensus, Diversity, and Learning in Organizations.* Organization Science, 1994. **5**(3): p. 403-420.
[35]. Walsh, J. and G. Ungson, *Organizational Memory.* Academy of Management Review, 1991. **16**(1): p. 57-91.
[36]. Klein, J., *Parenthetic Learning in Organizations Toward the Unlearning of the Unlearning Model.* Journal of Management Studies, 1986. **26**(3): p. 291-308.
[37]. Morgan, G., *Images of Organizations*. 2nd ed. ed. 1997, California, London, New Delhi: Sage Publications, Inc.
[38]. Hansen, M., *The Search-transfer Problem: The Role of Weak Ties in Sharing Knowledge Across Organization Subunits.* Administrative Science Quarterly, 1999. **44**(1): p. 82-111.
[39]. Nonaka, I., *A Dynamic Theory of Organizational Knowledge Creation.* Organizational Science, 1994. **5**(1): p. 14-37.
[40]. Ashford, B.E. and F.A. Mael, *Social Identity Theory and the Organization.* Academy of Management Review, 1989. **14**(1): p. 20-39.
[41]. Cybulski, J.L., et al. *Understanding Problem Solving in Requirements Engineering: Debating Creativity with IS Practitioners*. in *Proceedings of the Seventh*

Pacific Asia Conference on Information Systems. 2003. Adelaide, Australia: University of South Australia.
[42]. Stasser, G. and W. Titus, *Effects of Information Load and Percentage of Shared Information on the Dissemination of Unshared Information During Group Discussion.* Journal of Personality and Social Psychology, 1987. **53**: p. 81-93.
[43]. Argote, L., et al., *Group Learning Curves: The Effect of Turnover and Task Complexity on Group Performance.* Journal of Applied Social Psychology, 1995. **25**(6): p. 512-529.
[44]. Walsh, J.P., C.M. Henderson, and J. Deighton, *Negotiated Belief Structures and Decision Performance: An Empirical Investigation.* Organizational Behavior and Human Decision Processes, 1988. **42**: p. 194-216.

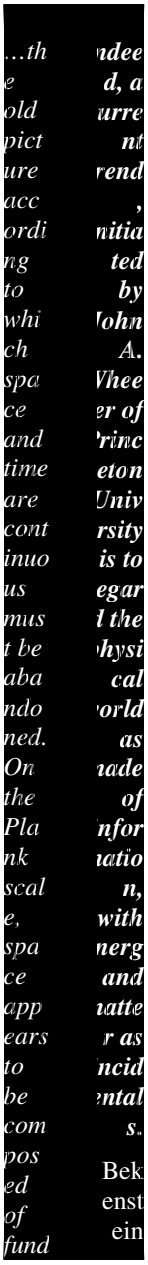
COPYRIGHT

Information Ethics: The Metaphysical Home of Computer Ethics

Karen Mather

Centre for Applied Philosophy and Public Ethics, and
School of Information Studies,
Charles Sturt University, Australia.

kmather@csu.edu.au



ame (20
ntal 03,
disc p.59
rete)
unit
s.

Sm
olin
(20
01,
p.16
9)

–

Abstract

Research in theoretical physics currently suggests that the basic fabric of the universe is not material: it is informational. This startlingly unorthodox claim concerning the nature of reality corresponds to an equally controversial ontological position found in the Floridian theory of Information Ethics. Increasingly, scientists in other fields, too, including computer science, seem to be articulating the belief that, in their fields, information is integral to what it means to have "being". In this paper, the information technologist's technique of Object Oriented Analysis is employed to provide a simple demonstration of the method by which objects can be seen as informational objects. The mounting appreciation of the fundamental importance of information coincides with the claim of Information Ethics that, as informational objects, all entities have some intrinsic value and are deserving of a minimalist moral consideration. This leads to wondering whether Information Ethics may be seen to provide a new metaphysical principle, "informationalism", as a companion to the traditional principles of materialism and idealism.

Keywords

Computer Ethics; Floridi; Fredkin, Holographic Universe; Information Ethics; Metaethics;; Object Oriented Analysis; Smolin.

INFORMATION SEEN AS THE BUILDING BLOCKS OF THE UNIVERSE

For the purposes of the following discussion, it is important to put aside the everyday meanings of the term "information" as the content of human communication. The setting here is one wherein theoretical physics and classical metaphysics are concerned with the most primitive elements of existence. At this level, scientists seek knowledge of the fundamental building blocks of the universe, whilst philosophers search for the ultimate answer to the question "what is there?" As will be discussed, in the 21st Century the advances in the state of knowledge about the natural world seem to result in all the answers to the questions about existence pointing to the conclusion that what every object has in common is that it is informational, whether the object be material (spatio-temporal), abstract, or even thinkable-but-impossible, as in Meinong's theory of objects (Lambert, 1995). This is the ground upon which this paper claims that, by considering every object that it is possible to refer to as an informational object, one may be positing informationalism as a metaphysical principle that cannot be subsumed into the principles of either materialism or idealism.

THE SIGNIFICANCE OF IE AND THE STRUCTURE OF THIS PAPER

> *Information Ethics is an ontocentric, patient-oriented, ecological macroethics*
> (Floridi, 2005, p.9).

This paper is the first deliverable from a research project that will reach completion several years from now. Thus, the paper's conclusion is still highly tentative and serves mainly to indicate the direction for continuing research. The argument begins to work towards examining the claim that Information Ethics (IE), as propounded by Floridi and his colleagues in the Information Ethics Group at Oxford, is a new metaphysical theory, rooted in classical metaphysical principles but, in understanding and implications, the philosophical counterpart of the modern revolution in scientific thinking. The overall significance of the IE position is that it claims to be a macroethical theory that is the philosophical foundation of the discipline of Computer Ethics (Floridi, 1999). As a macroethics, IE is not limited to one discipline in its applicability. Further, the minimalist moral worth that IE attributes to all entities provides the world-wide perspective that was sought by Gorniak-Kocikowska (2001) when she appealed for a new global system of ethics because "all ethical problems will eventually be problems of computer ethics" (Gorniak-Kocikowska, 2001, p.8). However, IE effectively inverts Gorniak-Kocikowska's view, and implies that any ethical problem may have an Information Ethics angle, whether computers are involved in the dilemma or not.

The paper begins with reference to the current literature of physics, particularly in relation to "the holographic principle" and its significance for an informational view of existence. The opinions of biologists are also included for consideration, since bioinformatics is at the forefront of innovative work in biology. The method of Object Oriented modelling is then employed to elucidate the way in which entities of any type can be represented informationally. Finally turning to metaphysics, the paper alludes to the views of certain philosophers on the metaphysical question of how to tell what there is in the universe, and in the light of how IE treats that question. This leads to the conclusion as to whether it will be rewarding to continue this line of research into IE and its claim to be an ontologically-based theory which posits that it is wrong to harm informational objects.

INFORMATIONALISM IN THE LITERATURE OF SCIENCE

In his keynote address to the 2005 European Computing and Philosophy Conference, Chaitin refers to the research of cosmologists, such as Smolin, Bekenstein and t'Hooft, who, he explains, are examining the possibility that the world could be built out of discrete information, namely binary digits. According to Smolin (2001), theoretical physicists' calculations appear to lead to the intriguing hypothesis that the universe is holographic: a three-dimensional image created from information stored in two-dimensions. A noteworthy characteristic of a hologram is that information about the whole is contained in all the parts: if a hologram of an object is bisected, both new holograms automatically contain all the original information (TWM, 2005).

Along this line of thought, Smolin (2001, p.178) adds that the research into String Theory, Quantum Gravity and M Theory strongly suggests that the best explanation will depict the universe not as a single holograph, but as a network of holographs, each of which contains information about the relationships between all holographs. That model, in turn, conjures up the picture of the universe (that is, everything that exists) as a network of relationships between events, whose activities consists of exchanging information: "In the end, perhaps, the history of a universe is nothing but the flow of information" (Smolin, 2001, p.178). As to the feasibility of such a concept, according to Thomas (Physorg.com, 2004) "3D volume means reading and writing billions of bits at one time", and since these access speeds are confirmed by Chuang et al (1999), Smolin's suggestion does not seem to be entirely impracticable, whether or not it is credible.

When Bekenstein (2004, p.31) embarks on an explication of the theory pertaining to black holes, he acknowledges his inheritance from John A. Wheeler, the "Father of the black hole", by stating simply that "information is the key concept here, as emphasised by Ruffini and Wheeler". Consistent with the claim of IE, which posits evil as entropy, Bekenstein also explains that entropy is defined as the loss of information (as was thought to occur, for instance, when atoms entered a black hole, according to the Hawking model of black hole theory (Lloyd and Ng, 2004, p.36), but was falsified by the Horowitz-Maldacena model that predicts that the information will be beamed back out of the black hole as a result of the quantum-mechanical "entanglement" between particles.)

This very brief review of the conjecture of scholars in the field of theoretical physics can be summed up by another quotation from one of its leading scientists and most articulate spokespeople, Lee Smolin:

> *… the world is not made of stuff, but of processes by which things happen. Elementary particles are not static objects just sitting there, but processes carrying little bits of information between events at which they interact, giving rise to new processes.* (Smolin, 2001, p. 63-64)

As Bekenstein (2003, p.59) mentions, the study of biology has added to the body of evidence supporting the idea that information is fundamental to existence. James Heath, who is Elizabeth Gilloon Professor of Chemistry at the California Institute of Technology (CALTECH), maintained in a recent Australian Broadcasting Corporation radio program (*Predictive Genome Testing*, 2005) that: "biology over the last several years has become an information science, which means that you want to think about biology as levels of information from the most fundamental, which is DNA to the most crude, which is basically the environment you live in".

The example of DNA is particularly appropriate for the IE view that all objects can be considered as informational objects. Computers can be used to simulate the composition and structure of biomolecules because the all-important protein is "an informational biopolymer" (Bioinformatics, 2003) whose structure can be seen as having been created by a series of yes/no answers. Since this paper is being given at the conference of the Australian Institute on Computer Ethics, perhaps one may be forgiven for digressing briefly to recall the heart-warming story of a heroic programmer, James Kent. As is stated on the Bioinformatics web site:

> *James Kent was awarded the 2003 Benjamin Franklin Award for developing ``GigAssembler,'' a 10,000 line program that he wrote in a month and then used to assemble the public human genome fragments. This was accomplished before Celera Genomics was able to assemble their private genome,[thus] helping to keep the data in the public domain and unrestricted by commercial patents.* (Bioinformatics, 2003).

When James Kent gave an address in response to being honoured with the Benjamin Franklin Award, he used the following diagram that illustrates how DNA "computes" and why it can be seen as an informational object.

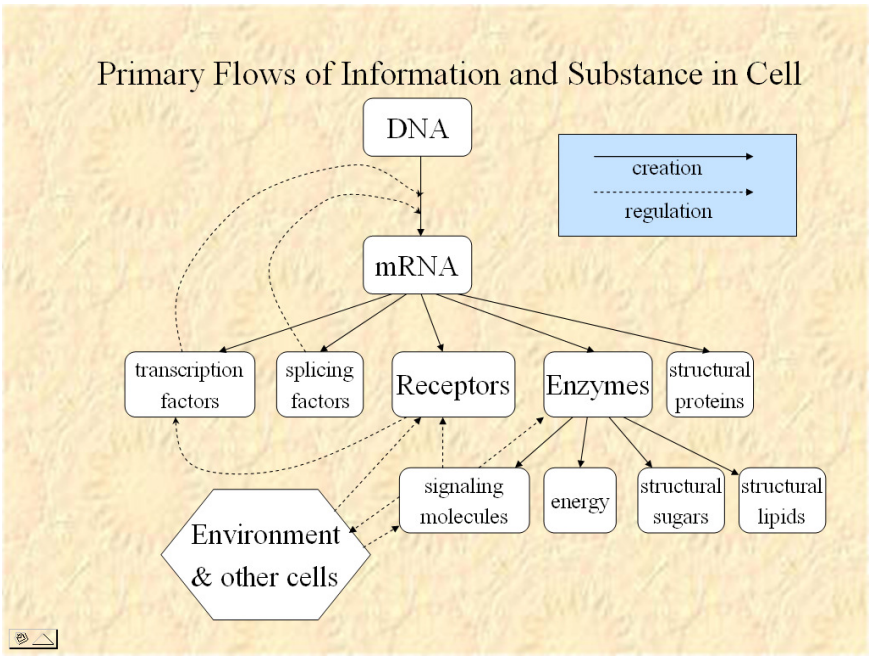


Figure 1. "Primary Flows of Information and Substance in Cell (Kent, 2003)

Figure 1 is a reminder of the claim of IE that, when conceptualising the most basic elements of what we know to exist, we find them to be composed of information. This is seeing information at a far more abstract level than the "aboutness" type of information which is used in everyday human life for purposes of description and other communication between people. Here, information is considered as primitive and essential; what all entities that exist have in common is the fact that, whatever else they may be, they are informational in nature.

The literature of Computer Ethics already records vigorous debate as to the plausibility of IE. And if IE is as important as it appears to be, this will soon develop into what Simon Blackburn (2005) refers to as a "splendid row"! Opponents of the theory (Mathiesen, 2004; Himma, 2005) doubt, amongst other things, the possibility of entities being informational objects. That objection appears to overlook the emergent understanding of information in the sciences, that information is a fundamental expression of existence. This objection is countered to some extent by the evidence that is issuing at a steady rate from the specialists who study the natural world (as has been shown above, very briefly). Perhaps an even more convincing proof is to be found in the theoretical framework that upholds the claims of IE. This theory is complex and draws on several other technical fields of theoretical knowledge. It has yet to be investigated by this project, and will form the subject of the next paper to be produced by the research.

BEING SEEN AS AN INFORMATIONAL OBJECT

A libertarian economist might argue, as an acquaintance once did, that to make provision for future generations is a failure to respect a tenet of economic reasoning, which holds that interference in market forces is questionable if not actually wrong. However, by looking at future generations as informational objects and using the method of Object Oriented Analysis to illustrate this, it is possible to see why future generations are worthy of more consideration than certain people may wish to accord them.

The example in Figure 2 illustrates a class of object known as the Human Race. This class has two sub-classes: 1) Fully Functional Persons and 2) Less than Fully Functional Persons. These two sub-classes are exhaustive – any object in the class of Human Race must fall into one sub-class or the other. In compliance with the conventions of information object oriented analysis (OOA) in Satzinger & Orvik (2001), the "generalisation/specialisation" notation is used here to indicate that the sub-classes are taken to be specialised examples of the general class. Importantly, with this type of class, the sub-classes automatically inherit all the attributes of the general class, to which their own specialised attributes are then added.

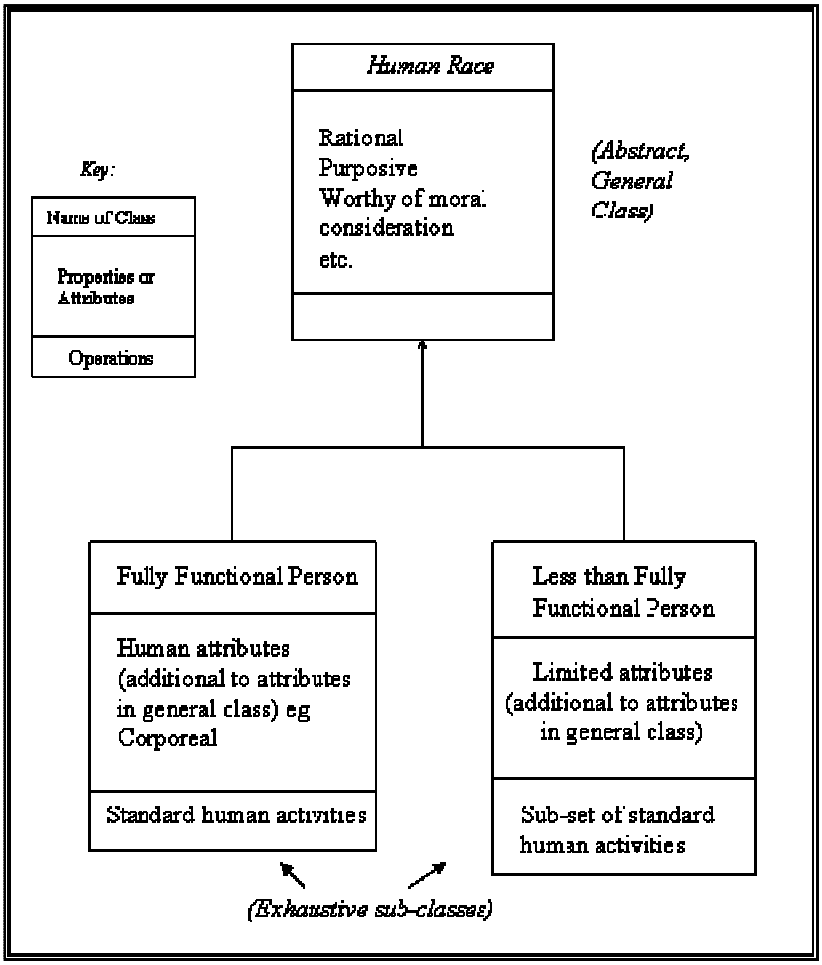


Figure 2. Object Oriented Diagram of Generalised/Specialised Relationships, based on Satzinger & Orvik, (2001, p.57)

By regarding future generations as members of the class of Human Race who fall into the sub-class of Less than Fully Functional Persons, the model indicates that these potential people automatically inherit the attributes of the main class of all persons, and thus are presently worthy of moral consideration – that is, their interests cannot rightly be disregarded now. This appears to explain the attitude normally adopted by people who care about their children, grandchildren and more distant descendants. As described by Mather (2005) this method of Object Oriented Analysis produces results that are consistent with the claims of IE to be an object oriented ethical principle.

Although all of the foregoing scientific opinion is important for an understanding of the way in which information can be seen as fundamental to existence, this is inadequate for a complete understanding of the claims of IE. It is clear from the work of Floridi and Sanders (2004) that full comprehension depends upon grasping IE's theoretical framework and what is meant by concepts such as "the level of

abstraction" (LOA) as applied in IE. On this point, notably, a straightforward hierarchy of diminishing detail or increasing simplicity is not the correct translation of LOA. So, it is the IE "take" on information theory combined with ontological theory and moral philosophy that underlies the claim of IE to be a guide to how human beings ought to implement their responsibility of stewardship of information.

SETTING OUT TO EXAMINE INFORMATIONALISM AS A METAPHYSICAL PRINCIPLE ("DIGITAL PHILOSOPHY")

Fredkin (2001) is credited by Chaitin (2004) with having coined the expression "digital philosophy", to describe how some contemporary philosophers and scientist now look at the fundamental processes of the universe in the new way described above. Chaitin also traces the beginning of this approach back to the philosopher Leibniz, who, in Chaitin's view, was the first to see the world as digital, created at the fundamental level by elemental choices of yes or no.

The dramatic question: "*Purquoi il y a plutot quelque chose que rien?"* (Eco, 2000, p.16) demanding why there is, more readily, something rather than nothing, was posed by Leibniz, who was "one of the most supreme intellects of all time" according to Bertrand Russell (1996, p.531). This question leads immediately to another: "how do we know that there is something?" after which it is a short step to the metaphysical question: "What does it take "to be"? Spinoza, a contemporary of Leibniz, famous for the systematic rigour of his metaphysical enquiry, provides a lucid description of the logical way to determine what fundamentally exists: "Whatever can be taken away from a thing without impairing its integrity does not constitute the thing's essence. But that whose removal destroys a thing constitutes its essence" (Spinoza, 2002, p.149, axiom number 2). This definition works well in the case of IE, which sees the damaging or removal of information as "entropy" and as threatening to the essence of an informational object.

Leibniz proposed that the final decision about what actually exists can be made by dint of pure logic. Most interestingly, Leibniz's logic led him to deduce that "space" is merely a system of relations (a view strongly reminiscent of the earlier-mentioned theoretical physicists' hypothesis that "Elementary particles are not static objects just sitting there, but processes carrying little bits of information between events at which they interact, giving rise to new processes" (Smolin, 2001, p.63-64).

The ancient Greeks understood that "the search for an understanding of Nature at a fundamental level in terms of basic processes and constituents necessarily carried them beyond the sensory world of appearance" (Drell, 1978). That is why, like Leibniz, Aristotle, too, employed reasoning to solve metaphysical problems, but, being also a scientist, Aristotle could base his reasoning on the habit of detailed study of the physical world. Nevertheless, the outcome of his deliberations was that the most indivisible primitive element of something that exists is what can only be referred to as "substance" or *ousia* (Aristotle, *The Metaphysics* book gamma, 1998). This much, Leibniz held in common with Aristotle, but Leibniz saw "substance" as immaterial, whereas to Aristotle a substance was (linguistically) that which is signified by a proper name, and presumably, therefore, not necessarily immaterial.

There are many towering figures in the history of metaphysics whose work is relevant to the question on hand, and no doubt the philosophy of science will prove a rich source of scholarly work with a very high relevance to the study of IE and the theory that supports its claims. For example, Floridi (1999, 2005) acknowledges the importance of the work of the scientist/philosopher, Norbert Wiener, as one of the progenitors of the theoretical position taken by IE. Beyond this, as mentioned, the Floridi-Sanders theoretical work awaits exploration.

CONCLUSION

It has been argued that some of the scholarly literature of physics and biology currently suggests that the universe (what is thought of as "reality") is informational in nature, and that this hypothesis is consistent with the Floridian theory of Information Ethics. The results of the research so far lead to the conclusion that IE appears to have an interesting and controversial position regarding the moral nature of information.

The research question that is driving the project asks whether Floridian Information Ethics entails a new metaphysical principle, namely "informationalism". Whatever the answer, the research will extend the current body of knowledge of Computer Ethics. It may result in Computer Ethics appearing to be a discipline-independent, applied ethics that conceptually has a strong relationship with the macroethical theory of Information Ethics. If that were to be the case, Computer Ethics would be endorsing the need to adopt an attitude of stewardship towards information, on the grounds that information is so much more than that which fuels computer systems.

ACKNOWLEDGEMENTS

Special thanks are due to Professor Luciano Floridi and Professor John Weckert who uncomplainingly made time to review this paper at extremely short notice. Their kind support is truly appreciated.

REFERENCES

Aristotle, 1998 *The Metaphysics*, Translated by Hugh Lawson-Tancred, Ringwood, Victoria, Australia: Penguin Classics.

Bekenstein, J. 2004 Black holes and information theory, *Contemporary Physics,* 45 1: pp. 31-43.

Bekenstein, J. 2003 Information in the holographic universe, *Scientific American, A*ugust 8th 2003, viewed on 13th August 2005 <http://www.sciam.com/article.cfm?chanID=sa006&articleID=000AF072-4891-1F0A-97AE80A84189EEDF>.

Bioinformatics Organization Inc. 2003 *Definition of bioinformatics: What is bioinformatics?* viewed on 10th August 2005, <http://www.sciam.com/article.cfm?chanID=sa006&articleID=000AF072-4891-1F0A-97AE80A84189EEDF>.

Blackburn, S. 2005 *Truth: A guide for the perplexed*, London: Penguin Books.

Chaitin, G 2005 Epistemology as Information Theory: From Leibniz to the Omega Number, Keynote speech at European Computing and Philosophy Conference, *Mälardalen University, 2-4 June 2005*, viewed on 1st August, 2005,< http://www.idt.mdh.se/ECAP-2005/>.

Chuang, E., Wenhai, L,. Drolet, J, Psaltis, D 1999 Holographic Random Access Memory. *Proceedings of the IEEE,* 8711: pp. 1931-1999.

Drell, S. 1978 When is a particle? The Richtmyer memorial lecture. *American Journal of Physics online,* 466: pp. 597-606, viewed 13th August 2005, <http://scitation.aip.org/getabs/servlet/GetabsServlet?prog=normal&id=AJPIAS000046000006000597000001&idtype=cvips&gifs=yes>.

Eco, U. 2000 *Kant and the platypus*, London: Vintage.

Floridi, L. 1999 Information ethics, its nature and scope. *Computers and Society* 345, viewed on 1st Augus 2005, <http://www.computersandsociety.org/sigcas_ofthefuture2/sigcas/subpage/sub_page.cfm?article=925&page_number_nb=1>.

Floridi, L. 1999 Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology,* 11: pp. 37-57.

Floridi, L. & Sanders, .J. 2004 The method of abstraction. M. Negrotti Ed. *Yearbook of the Artificial. Nature, Culture and Technology: Models in Contemporary Sciences*, Bern: Peter Lang: pp. 177-220.

Fredkin, E. (2001) Digital philosophy, viewed on 27th August 2005, <http://www.digitalphilosophy.org/digital_philosophy/toc.htm>.

Gorniak-Kocikowska, K. 2001 The global culture of digital technology and its ethics, *ETHICOMP 2001*, viewed on September 19, 2004, <www.ccsr.cse.dmu.ac.uk/journal/articles/gorniak_k_global.htm>.

Himma, K.2005. There's something about Mary: The moral value of things *qua* information objects. *Ethics and Information Technology*, 63: pp.145-159.

Kent, J. 2005 Slides from Dr. Kent's laureate seminar. Bioinformatics Organization Inc., viewed on 15 August 2005, <http://bioinformatics.org/franklin/2003>.

Kim, J. & Sosa, E. Eds. 1995 *A Companion to metaphysics.* Oxford: Blackwell.

Lambert, K. 1983 *Meinong and the principle of independence.* London: Cambridge University Press.

Lloyd, S.&.Ng. J.Y. 2004 Black hole computers. *Scientific American* 2915: pp. 31-39.

Mathieson, K. 2004 What is information ethics?. *Computers and Society*, 32 8, viewed on August 12, 2004, <www.computersandsociety.org/sigcas_ofthefuture2/sigcas/subpage/sub_page.cfm?article=909&page_number_nb=1>.

Mather, K. 2005 Object oriented goodness: A response to Mathiesen's 'What Is Information Ethics?'. *ACM Computers and Society,* 34 4, viewed on 1st August 2005, <http://www.computersandsociety.org/sigcas_ofthefuture2/sigcas/subpage/sub_page.cfm?article=919&page_number_nb=911>.

Physorg.com, 2004 Breakthrough nanotechnology will bring 100 terabyte 3.5-inch digital data storage disks, viewed on August 17 2005, <http://www.physorg.com/news785.html>.

Russell, B. 2004 *History of Western philosophy*. Routledge Classics, London: Routledge.

Satzinger, J. & Orvik, U, 2001 *The object oriented approach: Concepts, systems development, and modelling with UML*, Boston MA: Course Technology, Thompson Learning.

Smolin, L. 2001 *Three roads to quantum gravity*, New York: Basic Books.

Spinoza, B. 2002 Principles of Cartesian philosophy and metaphysical thoughts. Michael. L. Morgan, Ed. *Spinoza: Complete Works,* Indianapolis: Hackett Publishing: pp. 108-212.

Sullivan, A. 2005 US Officials go to hacker's convention to recruit. *Reuters.Know.Now* Reuters, viewed on 13th August 2005, <http://today.reuters.com/news/newsArticleSearch.aspx?storyID=266323+10-Aug-2005+RTRS>.

Predictive Genome Testing, 2005, *The Science Show:* radio program, ABC Radio National, Sydney, 28th May 2005.

TWM 2005 The universe as hologram. *Traditional Weather Modification Web Site,* viewed on August

10th 2005, <http://twm.co.nz/hologram.html>.

What is the difference between Transactional and Content data in an Internet Packet?

Darren Skidmore
University of Melbourne, Australia.

d.skidmore@unimelb.edu.au

Abstract

In the traditional meanings of telecommunications interception, there is a distinct physical separation between the transactional aspects of the communication call and that of the Content of that call. With communications sent via the TCP/IP protocol the separation of transactional and content data lapses. Another difference is that there is a blurring of the information which although is either used or is intended to be used as transactional information, can show up as content data. This paper looks at the issues of transactional and content data and why the TCP/IP and the Internet infrastructure are different to the old conventions of traditional POTS infrastructure.

Keywords

Transactional Data, Content Data, Interception, TCP/IP background.

INTRODUCTION

The origins of this paper came from reading the Council of Europe's Convention on Cybercrime[1], and concern about what the equivalent situation was under the Australian Legal system. Specifically the definitions of the types of data involved. In communication system there are two types of data, these are Traffic Data (also called Transactional Information) and Content Data, the distinction of which is particularly important in legal and ethical terms. At issue is the burden of proof to obtain a warrant for the later, which is Content information, and the fact that a communication stream over the Internet is vastly different from that of the traditional Telephone communication.

There is a difference between obtaining information which has been logged and obtaining information by interception, certainly under Australian law, the former requires a search warrant[2], whereas for the later, a Telephone Interception warrant has to be requested.

The second issue to deal with is the definitions of Traffic and Content data. Traffic data is the information collected by the communication system to set up, move and transfer the Content data. Traffic data for

[1] http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185

[2] Although the information may be provided without a warrant depending on the agency and the information required, under section 282(1) and (2) of the Telecommunications Act. This is discussed later.

example in a telephone call, is the number dialed, the originating number, date stamp and duration of the call. Content data, is the information that the two end parties[3] need to transfer, this could be a voice conversation, a pager message, the content of an email, or a document sent between two parties, it could also be a request by a computer to another computer, for example a Web service giving the a share price. Traffic data can include more information than required to make or conduct the communication, say for a telephone call all that is needed is the number dialed, however (usually for billing purposes) the date stamp of when the call was made, the duration of the call and the phone number which originated the call are seen as traffic data. Traditionally in telephony, it was very easy to separate the traffic data from the Content data, because of the nature of the communication network, the call was setup from one end to the other end, and then held in place until the call was terminated. The circuitry which setup the call was in most cases different to that which handled the transmission of the voice conversation. In the United States, the devices which are used to obtain the traffic data are called Pen Registers[4], in traditional telecommunication these would only record traffic data, therefore a warrant issued to obtain only traffic data could ensure that only traffic data was collected because of the limitations of the pen register, other separate equipment would be needed to obtain a warrant for a voice conversation (Content data). A very good example of the difference between traffic and content data is that of an envelope with a letter inside, what ever is written on the outside of the envelope could be considered to be traffic, the letter within the envelope however is content (this distinction may vary depending on the legal jurisdiction and this example is specifically from United States jurisprudence)[5].

In the United States and also in the Cybercrime Convention, a distinction is made between Traffic and Content data, however in Australia, no such distinction is explicitly recognized. In Australia a warrant for the interception of telecommunications is known as a Part IV warrant, which is issued under the Telecommunications (Interception) Act 1979 (Commonwealth)[6]. The warrants may be issued for Class 1 and Class 2 offences[7], they can also be issued as a "named" warrant rather than being aimed at a specific service, they are aimed at a specific person, and can be used for any service that is being used by that person. The Act does not give a definition for Traffic or Content data, rather a definition is given for communication, which is:

> "communication includes conversation and a message, and any part of a conversation or message, whether:
>
> (a) in the form of:
> (i) speech, music or other sounds;
> (ii) data;
> (iii) text;
> (iv) visual images, whether or not animated; or
> (v) signals; or
> (b) in any other form or in any combination of forms."[8]

The Australian Communications Authority has a fact sheet on Internet Service Providers Interception Obligations

---

[3]This can be person to person, or person to computer, computer to person, person to person via a computer network (best example would be email, a person sends the email to a computer, where the message waits, until the "intended" party logs on and retrieves the message).

[4]Berkowitz, Robert. "Packet Sniffers and Privacy: Why the No-Suspicion -Required Standard in the USA Patriot Act is Unconstitutional" Computer Law Review and Technology Journal Vol VII No 1. (Fall 2002) found at http://www.smu.edu/csr/articles/2002/fall/Berkowitz.pdf, visited 2003 Nov 10 [hereinafter Berkowitz, Robert 2002] Footnote 8 states "United Sates v Guglielmo, 245 F. Supp. 534, 535 (N.D. III. 1965) (explaining that a pen register is "a mechanical device attached on occasion to a given the phone line, usually at central telephone offices ... There is neither recording nor monitoring of the conversation.")."

[5]*id*. Page 2, including footnote 6 "see, e.g. United States v Huie, 593 F.2d 14, 15 (5th Cir. 1979) ("There is no reasonable expectation of privacy in information placed on the exterior of mailed items and open to view and specifically intended to be viewed by others.") "

[6]Part IV - Warrants authorising the Australian Federal Police to intercept telecommunications, the power can be delegated to state agencies as well. (Part VI Division 2 – Declaration of State Law Enforcement Authorities as Agencies)

[7]Class 1 Offences include murder, kidnapping, and narcotics (as well as aiding and abetting etc)
Class 2 Offences include offences punishable by imprisonment for at least 7 years, and involves a serious crime (the long list of Class 2 Offences are detailed in section 5D of the Act).

[8]Part IA – Interpretation, Telecommunications (Interception) Act 1979 (Commonwealth of Australia)

> "In practice, when served with an interception warrant, the ISP will be required to intercept all traffic transmitted, or caused to be transmitted, to and from the identifier of the target service ... used by the interception subject and described on the face of the warrant. ... The ISP must also provide access to the traffic-related data generated to process the traffic. For interception of Internet traffic, traffic-related data will be the signalling information contained within the IP datagram's and, where applicable, the calling line identifier of the telephone service used by the interception subject"9

Australian ISP's if the records exist must also give access to logs[10], customer details such as dynamically allocated IP addresses, log in / log out time total data transferred and the calling number, releasing them to a Law enforcement Agency (LEA) under Part 13 Telecommunications Act requests, warrants or court processes[11], also

> "[t]he "to" and "from" email address line of an email and any 'extended header' addressing information associated with routing a message from is originating point to its destination, is not content and /or substance of information"12

In the international arena, the current international treaty is the 2001, Council of Europe Convention of Cybercrime. Content Data is not defined, however Chapter I, Article 1 - Definitions

> d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

The problem is the last point of "underlying service". With an Internet communication, using a TCP/IP stream, it is reasonably easy to determine most of the Traffic / Transactional Data, and given a sufficiently programmed application or parser[13], the content could be removed, but this would be to the level of HTTP (or World Wide Web Traffic), FTP (File Transfer Protocol), DHCP (setup information for a computer when joining a new network or starting up), SMTP (Simple Mail Transfer Protocol). So it is possible to see what sort of traffic is being sent between two points, however there are issues with say for example email, you can tell if content is email, if the packet is using the SMTP protocol, however if the end user is using a Web Mail package, then the emails would be transported via HTTP packets[14]. In the case of Web Services[15], the transport of the content maybe SMTP, HTTP, or FTP but this would just be a wrapper transporting the Web Service remote procedure request, just using that Internet service to get from one computer to another across the network. The use of HTTP as a transport mechanism might also increase as the HTTP port[16] (generally port 80) is one of the few left open on the external (and possibly internal)

---

[9]Australian Communications Authority Fact Sheet: Internet Service Providers Interception Obligations FSI 12 6/2000

[10]There is no minimum time limit for the retention of records; however section 7.7 of the IIA Conduct code gives recommendations for personal data, 12 months, operational data (logins) 6 months and other data (Logs etc) 1 week after the creation of the record. The logs include Proxy logs, which give requesting IP address, time and the URI requested newsgroup logs, and ftp logs. Section 7.5 Internet Industry Association, "Internet Industry Cybercrime code of Practice – Codes for industry and self regulation and rules of engagement with law enforcement agencies in respect of investigation procedures regarding online fraud and other criminal and terrorist activity" [hereinafter referred to as IIA Conduct Code] Public Consultation Draft 2.0 July 2003 found at www.iia.net.au visited 2003 10 12

[11]Internet Industry Association of Australia, Fact Sheet, ISP disclosure requirements, accessed 2003 10 08 at http://www.iia.net.au/ispsheet.html, Australian Communications Authority Fact Sheet: Internet Service Providers and Law Enforcement and National Security FSI 12 11/2000

[12]IIA Conduct Code section 10.3

[13]A Parser is a program which goes through a document and strips out certain specified items, either giving you a file with those items or a file without those items.

[14]The best examples are Hotmail and Yahoo Mail services, but there are many other examples of this, the author uses Microsoft Exchange with outlook in the office, but will use the Web interface to Exchange when travelling.

[15] A Web Service is effectively a request by a computer to another computer to carry out a function; it could be to find out the time, to find out the current stock price of a company, options for a spell checker, the calculation of the correct tax on an invoice. Web Services can also be very complex, given sufficient permission and knowledge a Web Service could do your Holiday Season shopping.

[16]An Internet Protocol Address and a Port form a Socket, the computers use the socket to communicate with each other for each application, however for this paper a more technical description is not needed. Each application nominally listens to a different Port for communication, generally a Web Server listens to Port 80, a FTP service Port 20,21 and an Email Sever to Port 25, therefore if you

firewalls, as a security and workplace control measure. This means that the TCP/IP stream might need to be broken up to determine the nature of the information being transported.

AN INTERNET COMMUNICATION IS NOT A TELEPHONE CONVERSATION.

It is important to emphasis the differences between a communication over the Internet and a telephone conversation. This is because using an argument such as trying to describe the interception of Traffic data in Internet communications, as just being a Pen register is fundamentally flawed. In a traditional[17] telephone conversation, the call was setup, a permanent circuit then given to the conversation, the voice traffic could proceed between the parties, and circuit was not usable by any other person until the conversation was finished and the circuit dismantled. The setup is independent of the transport of conversation, and can be separated from the content of the call once the call has been setup.

With an Internet communication, there is no single circuit dedicated to a single communication, any communication is divided into many packets and each of these packets is sent from the source computer to the destination computer. In a packet delivery network any specific single packet can take any path from source to destination. There is also a difference between a circuit switched and packet switched network in that the content in the circuit switched call is just content, very little traffic data is needed for the conversation to proceed once it has been setup, however with packets each piece of content must contain traffic data, so that it can be transported from source to destination. This means that when viewing the packet for traffic data, the content is also present unless it has been stripped out, therefore any device referred to as a "Pen register" is actually capturing in the first instance, Transactional AND Content data, after which the content will be have to be stripped out. This is of course possible even in some cases trivial to do, however the physical separation provided by the traditional telephony is not available. Making analogies to a letter enclosed in a envelope, are not valid, a very apt description is that Internet packets are like postcards, where the addressing and content can be seen out in the open, however presumably even though the Intent communications act more like postcards, people using the Internet would probably expect the packets to work more like letters in envelopes.

WHAT IS TRAFFIC / TRANSACTIONAL DATA AND WHAT IS CONTENT?

Transferring from telephony to Internet communications, it is probably reasonable to map that the date / time stamp, is the same as for a phone conversation. The source and destination IP addresses, will map to the origin and terminating telephone numbers. Rather than duration of the data call, the size of the communication may map to the duration of the call, the duration of an Internet communication is dependent on the speed of the communications channel so the duration of the "call" will change depending on if it is a PSTN modem or a Broadband connection[18].

The size is different depending on which size is being referred to, the size of a packet is small, however, the content transmitted will be much larger, for example to download the United States Department of Justice web site, the initial packet size that makes the request is 495 bytes long, however the total size of the download was 67,701 bytes, the total number of packets in the communication was 96 packets, and the time between the first and the last packet was 5.737 seconds. See Table 2 for more details.

---

are running all these applications on one machine, if data comes into the machine on Port 80, the Web Server takes it and tries to interpret it, expecting HTTP traffic. Similarly if data is sent on Port 25, most applications would interpret it as SMTP or email traffic. Some times hackers / others will send information on other ports either to enter a system or to obscure the information, as it will be ignored due to being a Port not listened for by other applications. The source port is always the first two octets of the TCP packet and the destination port is the second two octets.

[17] I am using the word traditional here because it is becoming more common to either use the same infrastructure as the Internet communications or to use similar technologies, therefore the distinction between a telephone call made now and surfing a web page is becoming where one transports voice, and one text and pictures. The telephone calls do not include the use of Voice over IP technologies, as used on the Internet.

[18] For example I was recently sent a word document which was an invitation to a family event, the person sending it was on a 56k Dialup modem, the email containing the file (3.5 Mb) took ¾ of an hour to send, from their computer to their ISP. However when I sent it on to another family member, from my computer at work which is on a 100Mbs network, I did not notice any delay in the email being dispatched. For this reason it would be better to use size of the communication rather than time taken, although, the time taken might provide clues as to the type of transmission mediums.

The problem on the Internet is that even the simplest pieces of traffic data can reveal content information, some of which would be expected for example at the level of email addresses, which can state who a person is, and where they work. Similar to sending a letter, where you identify a person by name, title, perhaps work address, perhaps home address, this does not reveal anything about the content of the letter. A subject line, in an email might however reveal the content of the message, but is not considered traffic data.

A web page is slightly different, with a web page, the URI[19] revels a lot more information, the URI shows a destination, but also something about the content of the web page for example:

> http://**web.dis**.*unimelb.edu.au*/staff/**dazs/***research*/cybercrime.**php**
>
> This URI reveals quite a lot of information the server is the **web.dis** server, which is located within the domain of *unimelb.edu.au* (which is an Australian Educational facility[20]). The login of the staff member is **dazs,** and this is part of their *research*, into cybercrime, which is possibly a dynamically built web page (.**php**) rather than a static web page (would have been .html or htm)

Just the URI does not say anything about what the content of the web page actually is, but it does reveal some information, of course it is very unlikely that someone would name a URI:

> http://www.terroristsRus.com/instructions/bombs/nuclear/beginners/howtoenrichuranium.html

Beyond this a web page that is viewed by a person, has quite a lot of transactional information, the content that is viewed is made up of HTML tags, e.g.

> <title>DOJ: U.S. Department of Justice Home Page</title>

The text between the <title> HTML tags is the title of the home page, and is displayed in the Title bar of the URI, and is generally used to describe the page when book marking the URI. Although the whole text is content traveling over the Internet, the <title> tags are transactional information for the web browser.

The web page must not only download the text content from the USDOJ from the HTML document which is the homepage. As part of building the web page, there are also several images and text which must be obtained from other locations, i.e. the web page home.html, as part of loading requires that it downloads content from other locations. So the loading of the page creates further calls which generate traffic and content data. URI's can be actively used, but there are also passive URI's such as those used as possible links to select further web pages. Links are a URI which contain transactional information (i.e. Where to go, and how to do it, IF the link is clicked on) the URI does not become transactional until it is selected, until then it is merely content on the page.

There is other "transactional" data involved in a URI, when conducting a search there is transactional information that can be sent as part of the search string in the URI, e.g.

> http://**www.google.com/***search***?&q=Cybercrime+telephone+interception+warrants**

This is a google search to find information on Cybercrime plus information on Telephone Interception Warrants, to actually do the search the "**?&q=Cybercrime+telephone+interception+warrants**"is needed, however this is transactional data for the Web Server at google, not traffic data for the Internet, to transport the request over the internet the only thing needed is the **www.google.com** or to be more precise the IP address which is **216.239.39.99**, the directory to go to */search*, and the **?&q=Cybercrime+telephone+interception+warrants**, is actually part of the content that the web surfer wants to transact with Google. However (Berkowitz, R 2002 p6) discussing Smith v Maryland says the court reasoned that both dialing a telephone number and records conveyed to a bank to complete a transaction that "a person has no legitimate expectation of privacy in information he voluntarily turns over

[19]URI = Uniform Resource Identifier, (a URL or Uniform Resource Locator is a subset of a URI) points to resources on the Internet, usually this is referring to a web page, but they also point to pictures which are shared by several web pages, e.g. Bullet points, and company logos. They also point to songs, background music, and multimedia images, which are used in building web pages. They can also refer to Internet services which are not Web or Web related pages, e.g. Ftp servers, telnet connections.

[20]Care must be taken with the country codes e.g. A .au should indicate Australia, but Australian companies may not use Australian domain names, and companies based outside of Australia may use a .au domain. Although the .edu domain is generally enforced, in New Zealand, and England they use .ac (academic institution) instead of .edu, the .com's , .org's and .net's vary depending on the application rules of the domain registrar.

to third parties"21. So in this instance it might depend on if the web surfer is handing the information about the search string over to google, who performs a service in creating the web page of links for them (unclicked hyperlinks), or if the entire string is transferred to a third party (in the first instance to the ISP, then to the internet as a whole, all the way to the google web server). Taking the argument in reference to the dialed numbers or to the records for a banking transaction, the search string is not being transferred to the ISP for them to use; the ISP is given the IP address (translated from the domain name) for www.google.com. The question might be if google is a third party, because they are using the search string to create information for the web surfer. As can be seen in Table 1, the first line is a Get, which is a request to obtain the search string, however the Host is on the second line, which is at www.google.com, and although not shown in Table 1 the destination IP address is 216.239.39.99, which is the google server. In this case the URI placed into the browser has been divided by the browser in making the request (so at the computer before going out over the network) in to a request to the ISP (and Internet infrastructure) to send a message to 216.239.39.99 and part of this message (in the HTTP protocol) is to get information from the directory called search for information on Cybercrime telephone interception warrants.

Cookies are another transactional item that can be used in web pages, in building a dynamic web page for a customer (say Amazon.com) where they check to see if you have an amazon.com. cookie, and if they find one they will personalize the page they present to you. When you request a page from Amazon, Amazon checks to see if a cookie has been set on your machine, if so then it retrieves that cookie and uses it to match that cookie so they can personalize the page to the entity using the browser. Again this is a transactional piece of information that is content rather than traffic data.

The examples Table 2 and Table 3 are of captured examples of captured TCP/IP streams; they describe some of the aspects discussed above, and show the raw HEX characters which are set over the Internet, with translations of the some relevant aspects. If we look at the first two lines on both of them which is the Internet Protocol and the Transmission Control Protocol sections, we can determine a lot of information.

In the Internet Protocol section, the 10th byte tells us that the following data is TCP data (other options include UDP packets, or control information), the last 8 bytes give the source and destination addresses of the packet, they are the same for both examples, except for the destination address of the FTP because this is a different server, the source address is the same because all testing was done from the one computer..

In the Transmission control packet, the first 4 bytes say what type of service is going to be running, based upon the destination Port, we can see that in Table 2 which is the web page, the HTTP protocol is going to be used (port 80 or 00 50 in Hex) whereas in Table 3, which shows a File transfer, the protocol is FTP (Port 21 or 00 15 in Hex). Although in both these examples the IP header and the TCP header were the same length, this is not always the case, and although generally the IP/TCP header is 40 bytes in length, this can vary.

However as can be seen from the capture, you must scan the whole packet, indeed you must scan the complete stream (all 96 packets out of 195 packets) to get the whole page, and because the web page is broken into multiple small packets, the first HTTP packet informed the scanner what was being requested, the other 60 HTTP packets were just the content being transferred. If there had of been multiple web pages being loaded at the same time, say 5, then 5 packets would have been requesting 5 web pages, but there would have been 305 packets using the HTTP protocol. Because of the nature of TCP, all 5 could be distinguishable even if they were going to the same web site, or even if they were going to the same page, however you would need to break open the TCP/IP stream a bit further to determine which packets belonged to which web page. This is where real time capture would assist, in determining content, especially if the page was dynamically built. With a static page, an investigator would be able to view the web page merely by typing in the URI: and visiting the page. However where a web page is dynamically built, or is protected by a cookie, the web page (or file) could only be rebuilt if captured using the appropriate software, and then reassembled.

In the research for this paper, a capture of a email was made, one using the Email client Outlook Express and the other using a Hotmail account. Using Ethereal[22] it was extremely simple to view and find the

[21] Berkowitz, R 2002, page 6, quote comes from Smith v Maryland, 442 U.S. 735 (1979) at 743-744

[22] Ethereal is a packet sniffer program widely available on the internet, that can capture and view a wide range of network information, including TCP/IP traffic

related TCP/IP packets of both emails. The email sent using Outlook express could be seen and reproduced easily, however the email on the hotmail account was much harder to distinguish as it was reproduced along with the html tags for marking up the web page, the associated links and pictures which were part of the Hotmail advertising. However a more sophisticated program may possibly be able to extract that information.

CONCLUSION

The growth in TCP/IP traffic is extending as more and more people use the internet and as more an more applications use the TCP/IP protocols, given that to intercept the transmission of data in real time, is to capture, both transactional and content data, and the ease with which this can take place, care should be taken in the issuing and terms of Telephone Intercept Warrants. The log files which are kept on transactions are also very revealing about peoples activities on where they go, what they do, perhaps a higher burden of proof should be required for these, especially if several of the disparate log files are connected together to put a profile of the user of the equipment.

This paper has tried to look at some of the issues in relation to TCP/IP traffic being captured, and the nature and meaning of the packets, along with the risks, as well as why it is not appropriate to consider that Internet communication can simply be considered similar to telephone communication in terms of the separation of transactional from content data.

REFERENCES:

Australian Communications Authority Fact Sheet: Internet Service Providers Interception Obligations FSI 12 6/2000

Berkowitz, Robert (2002). "Packet Sniffers and Privacy: Why the No-Suspicion -Required Standard in the USA Patriot Act is Unconstitutional" Computer Law Review and Technology Journal Vol VII No 1. (Fall 2002)

CyberCrime Convention. http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185

Internet Industry Association of Australia (2003). Internet Industry Cybercrime code of Practice – Codes for industry and self regulation and rules of engagement with law enforcement agencies in respect of investigation procedures regarding online fraud and other criminal and terrorist activity. Public Consultation Draft 2.0 July 2003 at www.iia.net.au visited 2003 10 12

Internet Industry Association of Australia (2003), Fact Sheet, ISP disclosure requirements, Australian Communications Authority Fact Sheet: Internet Service Providers and Law Enforcement and National Security FSI 12 11/2000 at http://www.iia.net.au/ispsheet.html, accessed 2003 10 08

Telecommunications (Interception) Act 1979 (Commonwealth of Australia)

United States v Huie, 593 F.2d 14, 15 (5th Cir. 1979)

TABLES

Table 1 : Translation of TCP / IP single packet in the stream showing the search request to Google for Cybercrime telephone interception warrants

GET /search?&q=Cyberc rime+te leph

one+interception+warrants HTTP/1.1 Host: www.google.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20030925 Accept: text/xml, application/xml,application/xhtml+xml, text/html;q=0.9,text/plain;q=0.8

,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=3b1997646 84c70f6:


CR=
1:T
M=1
0562
4788
1:L
M=1
0562
4788
1:S=
jB4e
3ubh
Q2ii
7xpJ
Prag
ma:
no-
cach
e
Cac
he-
Cont
rol:
no-
cach
e

_Table 2: Example of getting a Web Page www.usdoj.gov

This is the first main packet of the downloading of the main United States DoJ web home page, the entire web page took 96 packets and

took 74,323 bytes, 5.737 seconds from the first to the last packet, while it was being loaded a further 99 packets were sent and received on the

Network Card that was being used, with 121,958 bytes of traffic in total.
Internet Protocol Section
Protocol == *06* == TCP
Source

–
*80
f1
6f
d6*
=
128
.25
0.1
11.
214

esti
nati
on:
*90
65
01
20*
=
149
.10
1.1.
32

*
Not
e
the
des
tina
tio
n is
the
ww
w.u
sdo
j.g
ov
site
as
this
is
the
req
ues

t for the web page, when the US DoJ was actually sending the HTML page to the computer the source and destination were reversed.

f

the data, 61 of the 96 (63.5%) packets were HTTP (sending Web data), and 35 of the 96 (36.5%) were TCP (acknowledging receipt and control

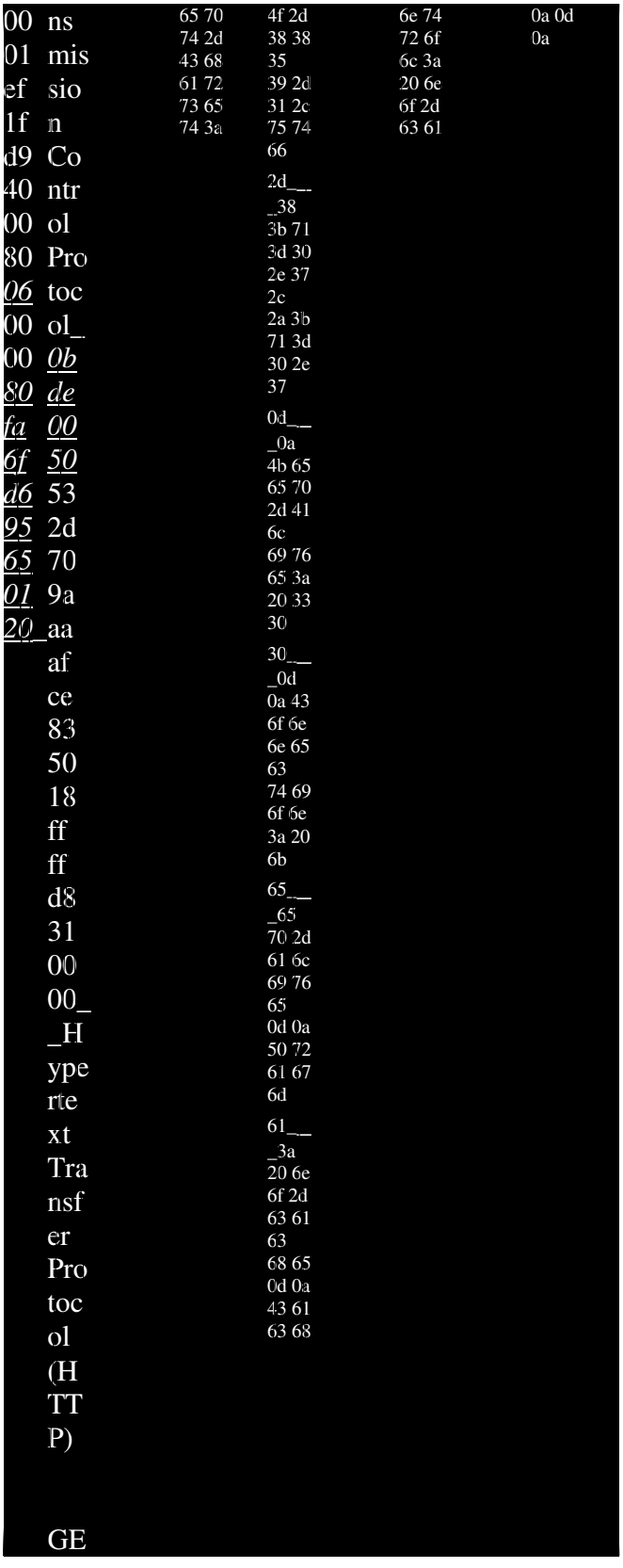
messages between the two ends)

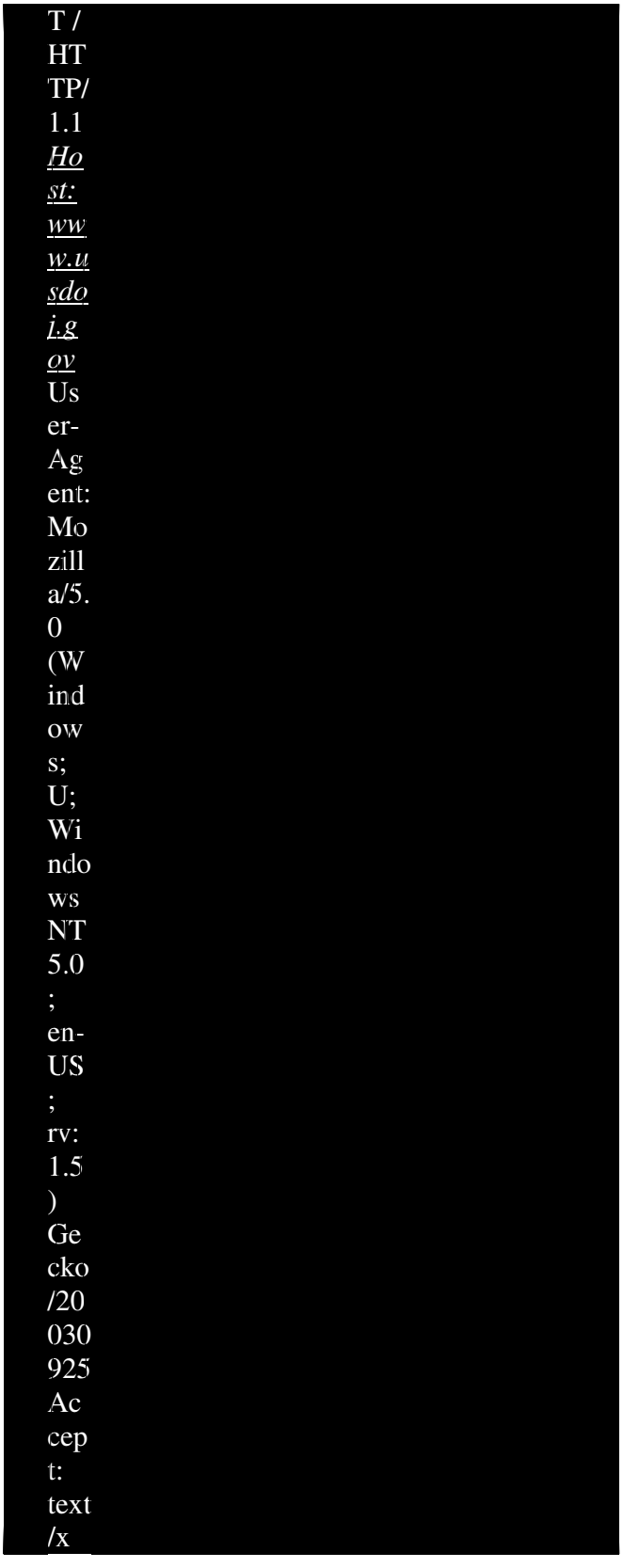
TCP Header:

Source Port: *0bde* =3038

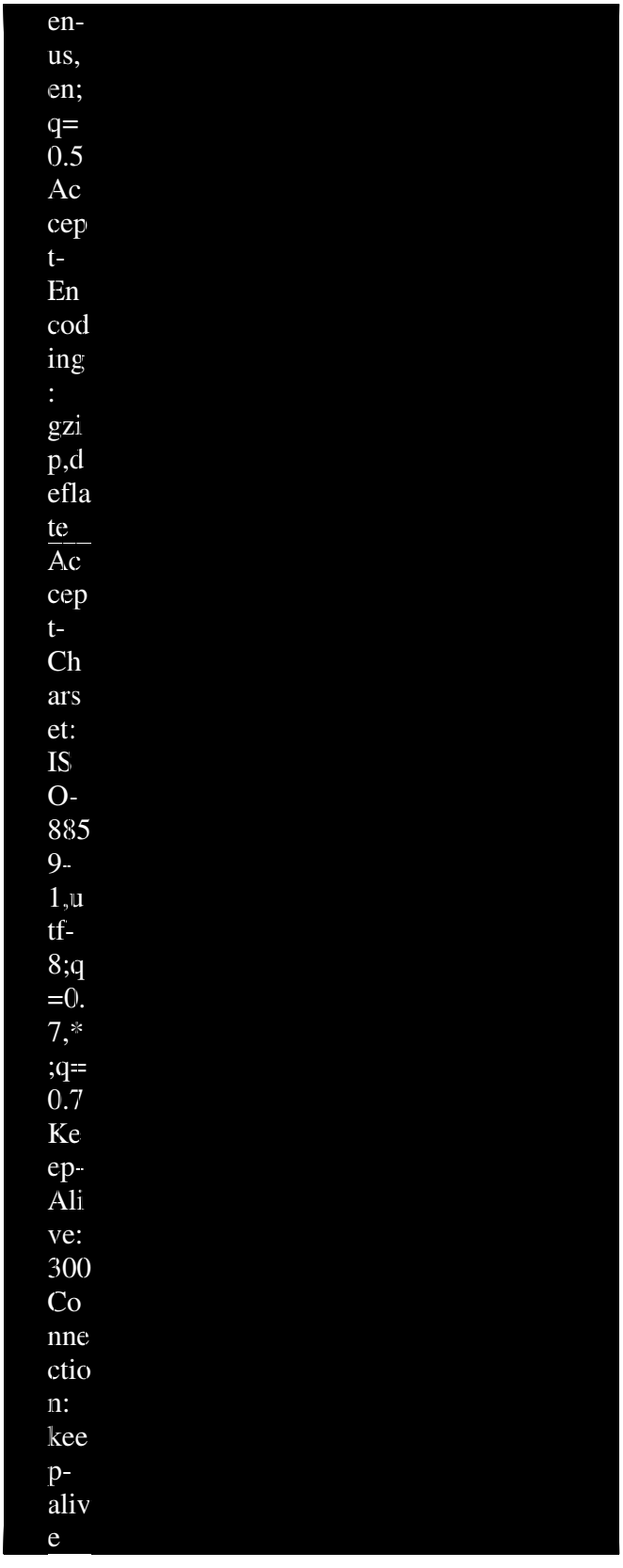
Destination Port: *0050* = 80 (*HTTP*)

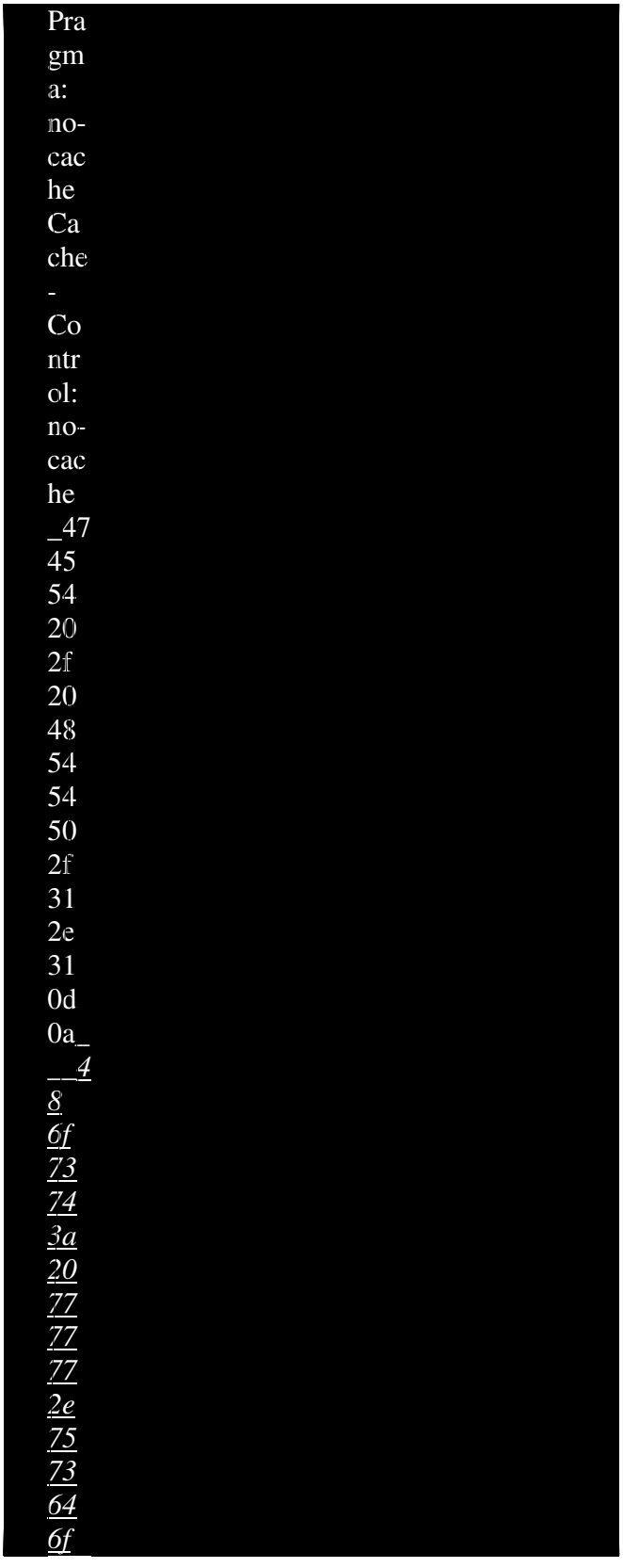
Internet Protocol 45

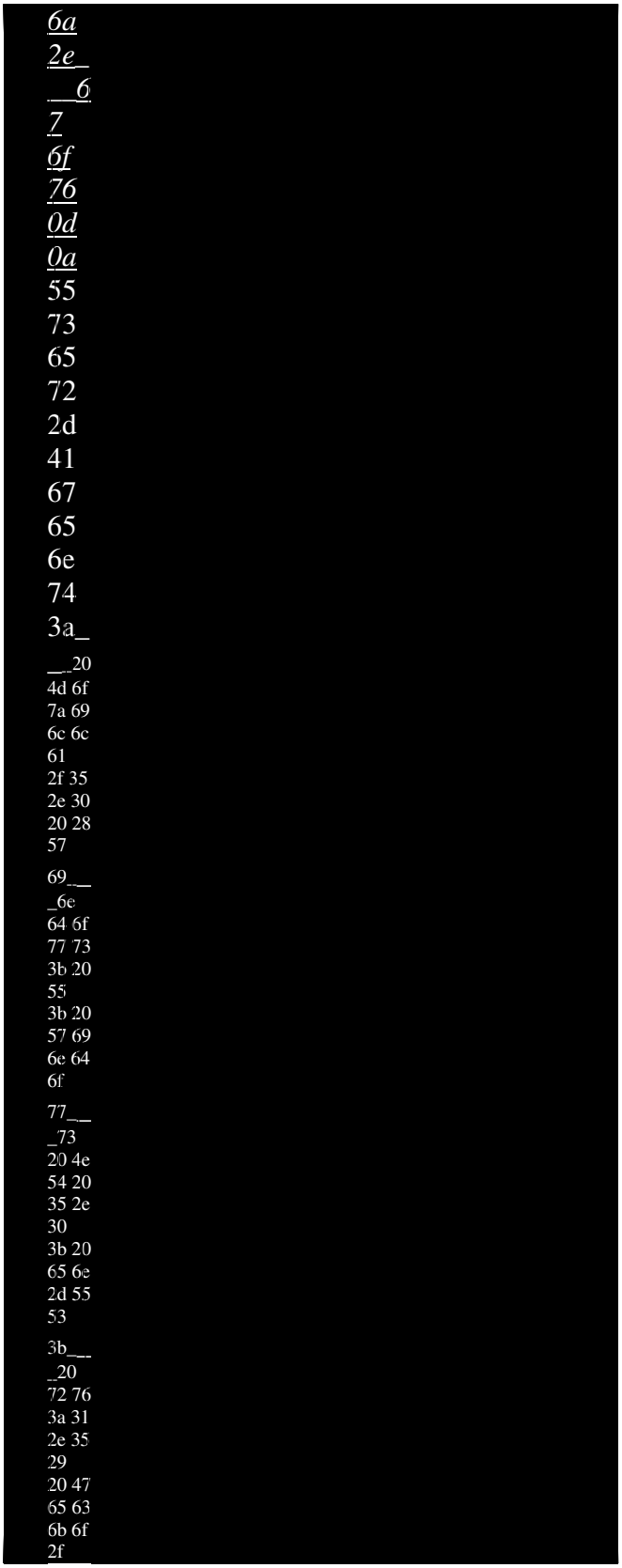

00 ns 65 70 4f 2d 6e 74 0a 0d
01 mis 74 2d 38 38 72 6f 0a
ef sio 43 68 35 6c 3a
1f n 61 72 39 2d 20 6e
d9 Co 73 65 31 2c 6f 2d
40 ntr 74 3a 75 74 63 61
00 ol 66
80 Pro 2d__
06 toc _38
00 ol_ 3b 71
00 0b 3d 30
80 de 2e 37
fa 00 2c
6f 50 2a 3b
d6 53 71 3d
95 2d 30 2e
65 70 37
01 9a 0d__
20 aa _0a
af 4b 65
ce 65 70
83 2d 41
50 6c
18 69 76
ff 65 3a
ff 20 33
d8 30
31 30__
00 _0d
00_ 0a 43
_H 6f 6e
ype 6e 65
rte 63
xt 74 69
Tra 6f 6e
nsf 3a 20
er 6b
Pro 65__
toc _65
ol 70 2d
(H 61 6c
TT 69 76
P) 65
0d 0a
50 72
61 67
6d
61__
_3a
20 6e
6f 2d
63 61
63
68 65
0d 0a
43 61
63 68
GE

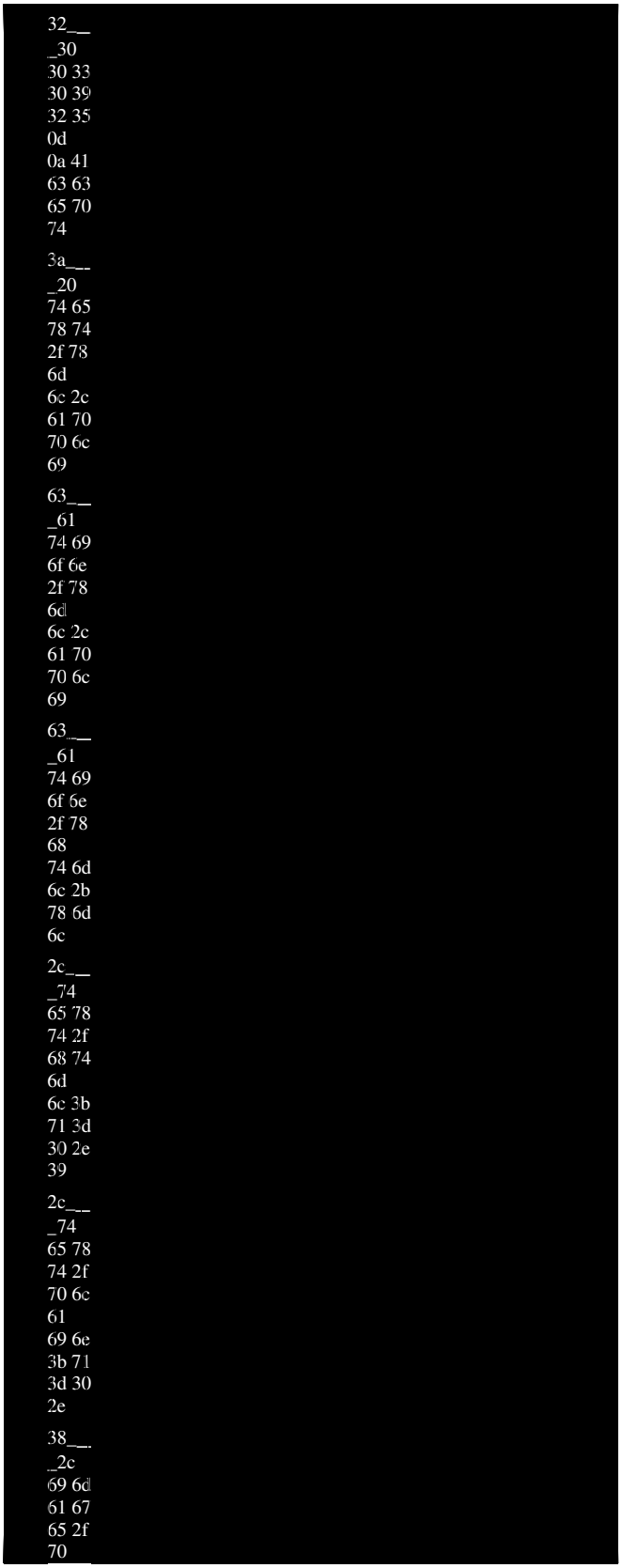

T /
HT
TP/
1.1
Ho
st:
ww
w.u
sdo
j.g
ov
Us
er-
Ag
ent:
Mo
zill
a/5.
0
(W
ind
ow
s;
U;
Wi
ndo
ws
NT
5.0
;
en-
US
;
rv:
1.5
)
Ge
cko
/20
030
925
Ac
cep
t:
text
/x

ml,
app
lica
tio
n/x
ml,
app
lica
tio
n/x
ht
ml
+x
ml,
text
/ht
ml;
q=
0.9,
text
/pla
in;
q=
0.8,
ima
ge/
png
,im
age
/jpe
g,i
ma
ge/
gif;
q=
0.2,
/
;q=
0.1
Ac
cep
t-
La
ngu
age
:


en-
us,
en;
q=
0.5
Ac
cep
t-
En
cod
ing
:
gzi
p,d
efla
te
Ac
cep
t-
Ch
ars
et:
IS
O-
885
9-
1,u
tf-
8;q
=0.
7,*
;q=
0.7
Ke
ep-
Ali
ve:
300
Co
nne
ctio
n:
kee
p-
aliv
e


Pragma: no-cache
Cache-Control: no-cache
_47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a_
__4 8 6f 73 74 3a 20 77 77 77 2e 75 73 64 6f


6a
2e_
__6
7
6f
76
0d
0a
55
73
65
72
2d
41
67
65
6e
74
3a_
__20
4d 6f
7a 69
6c 6c
61
2f 35
2e 30
20 28
57
69__
_6e
64 6f
77 73
3b 20
55
3b 20
57 69
6e 64
6f
77__
_73
20 4e
54 20
35 2e
30
3b 20
65 6e
2d 55
53
3b__
_20
72 76
3a 31
2e 35
29
20 47
65 63
6b 6f
2f


32_
_30
30 33
30 39
32 35
0d
0a 41
63 63
65 70
74
3a_
_20
74 65
78 74
2f 78
6d
6c 2c
61 70
70 6c
69
63_
_61
74 69
6f 6e
2f 78
6d
6c 2c
61 70
70 6c
69
63_
_61
74 69
6f 6e
2f 78
68
74 6d
6c 2b
78 6d
6c
2c_
_74
65 78
74 2f
68 74
6d
6c 3b
71 3d
30 2e
39
2c_
_74
65 78
74 2f
70 6c
61
69 6e
3b 71
3d 30
2e
38_
_2c
69 6d
61 67
65 2f
70

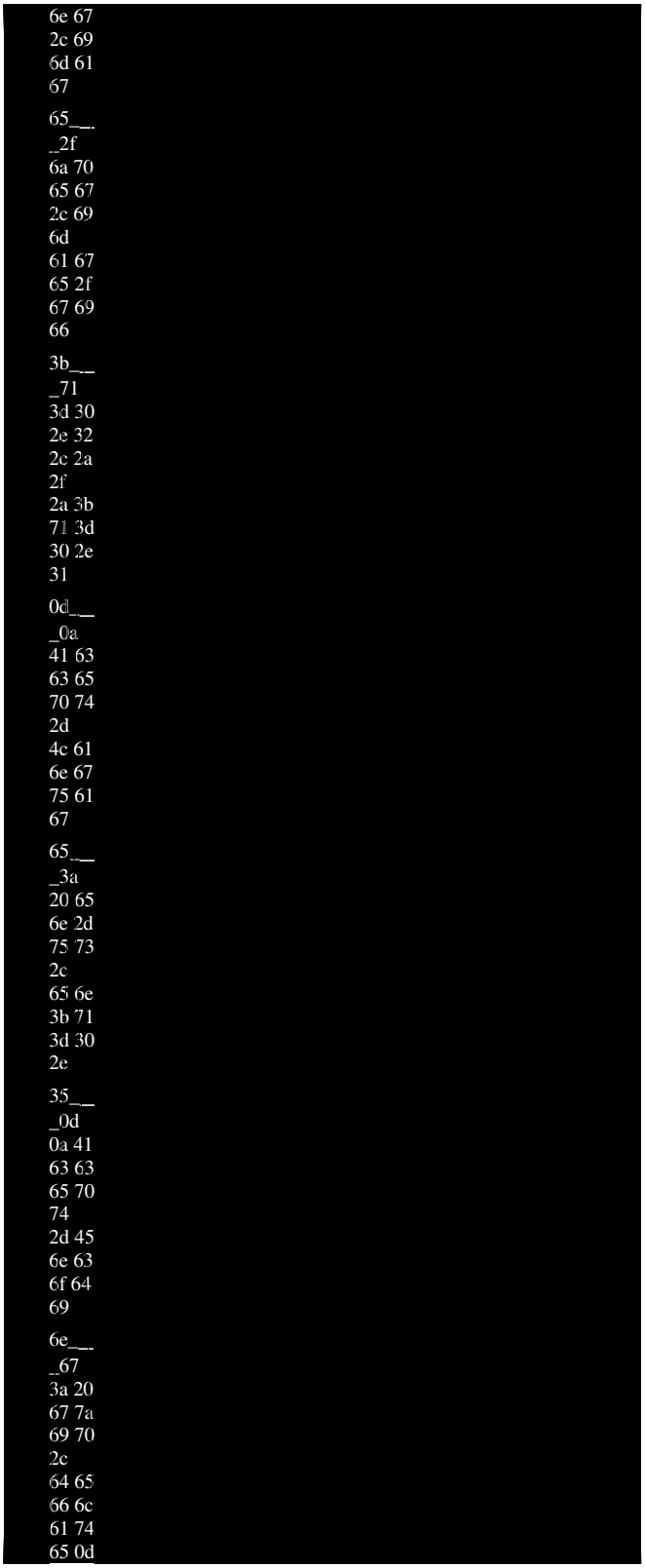

6e 67
2c 69
6d 61
67
65_._
_2f
6a 70
65 67
2c 69
6d
61 67
65 2f
67 69
66
3b_._
_71
3d 30
2e 32
2c 2a
2f
2a 3b
71 3d
30 2e
31
0d_._
_0a
41 63
63 65
70 74
2d
4c 61
6e 67
75 61
67
65_._
_3a
20 65
6e 2d
75 73
2c
65 6e
3b 71
3d 30
2e
35_._
_0d
0a 41
63 63
65 70
74
2d 45
6e 63
6f 64
69
6e_._
_67
3a 20
67 7a
69 70
2c
64 65
66 6c
61 74
65 0d

_Table 3: Example of an FTP transfer of a file

This is the first main packet of the downloading by FTP a file called Read Me .Txt from the University of Melbourne FTP site. (There were

two sessions, this one which requested and confirmed finish, and the second which transferred the data. The file is 38.7 Kbtyes, This transaction

took 9 packets and took 714, bytes, 0.388 seconds from the first to the last packet.

The data transfer transaction took 50 packets and took

42,
395
byt
es,
0.2
60
sec
ond
s
fro
m
the
firs
t to
the
last
pac
ket.
Wh
ile
bei
ng
loa
ded
a
furt
her
15
pac
ket
s
wer
e
sen
t
and
rec
eiv
ed
on
the
Net
wo
rk
Car
d

that was being used, with 45,444 bytes of traffic in total. Internet Protocol Section

Protocol == *06* == TCP

ource --*f16fd6* = 128

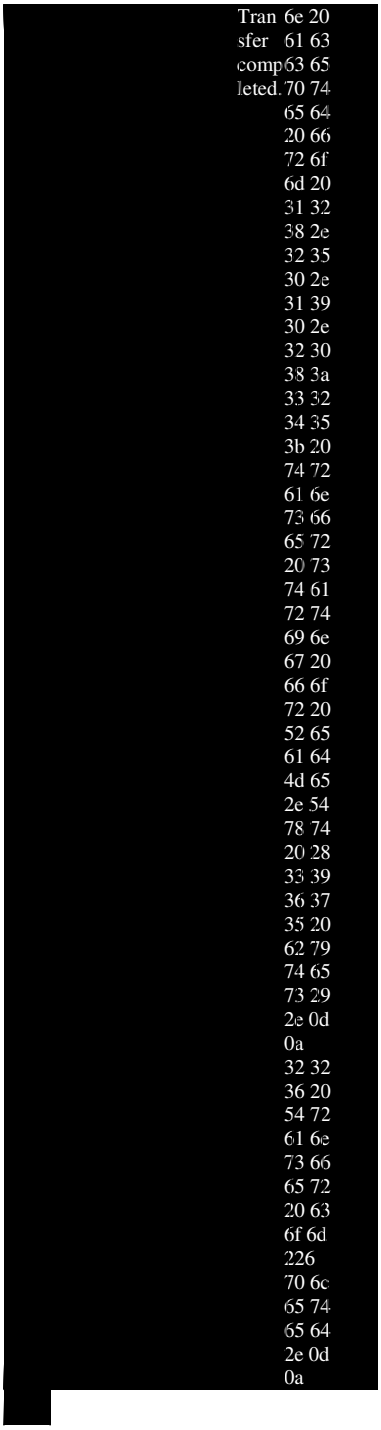
.25
0.1
11.
214

esti
nati
on:
*80
fa
14
31*
=
128
.25
0.2
0.4
9
TC
P
He
ade
r:

So
urc
e
Por
t:
*0c9
b*
=3
227

De
stin
atio
n
Por
t:
*00
15*
=
21
(*FT
P*)

Int
ern
et
Pro
toc
ol
45
00
00
30
54
88
40
00
80
06
00
00
80
fa
6f
d6
80
fa
14
31



–

COPYRIGHT

Privacy, Surveillance and the Australian State: Law and Computer Ethics in a Post-September 11 World

Ian Harriss
Charles Sturt University, Albury, Australia.

Abstract
Privacy is a concept that is philosophically vague and legally weak in the Australian common law. Considered in philosophical terms, the issue has been bedevilled by spatial, bodily and proprietary concepts. Consequently, as far as privacy is concerned, the technological realities of contemporary society remain largely unaddressed by the common law. Recent legislation emerged from that tradition. The legislation contains a number of important exemptions; it is based on vague concepts of fair dealing; and the system is a complaints-based one.
Thus, the legal regimes that attempt to address privacy are deeply flawed. They are fragmentary, reactive and very difficult to enforce. Meanwhile, threats to privacy and data security multiply as technological change creates more privacy-invasive opportunities. This is particularly so in the post-September 11 world. Arguably, parallel regimes are emerging: one for 'normal' citizens, and another for those of interest to the anti-terrorist organs of the State. The first regime needs strengthening, and the second needs checks and safeguards.
Encryption enhances privacy, but in the contemporary climate it conflicts with the interests of the State. The ethical issues need to be clarified before they can be resolved.

Keywords: Privacy, surveillance, ethics, data.

INTRODUCTION: PRIVACY AND THE STATE

In this paper I argue that the Australian law relating to privacy is in a state of confusion and contradiction in the post-September 11 world. There are now two divergent streams, each with its own paradigm, and each with its own history and trajectory: there is a weak statutory regime developed from a weak and fragmented common law tradition; and there is a second stream, legitimised in the age of terror, that seeks to use the technology of a surveillance society in order to enhance collective security.
The first stream, which is based on nineteenth century conceptions of the liberal autonomous individual, fails in fundamental ways to protect individuals in the workplace and in society at large. The legislative regime is a complaints-based framework based on vague concepts of fair dealing, and it contains so many exemptions that its supposed purpose is effectively negated. Moreover, the legislation is contained in numerous Acts at both State and Commonwealth level (*Privacy Act (Cth) 1988; Privacy Amendment (Private Sector) Act (Cth) 2000*; *Information Privacy Act (Vic) 2000;* W*orkplace Video Surveillance Act 1998 (NSW);Surveillance Devices Act 1999 (Vic)).*
Such a mish-mash has emerged from a common law in which there is no right to privacy as such: instead, at common law threats to the integrity of the individual are conceived in terms of boundaries that protect the bodily integrity, and the public character, of the

individual from external invasions. The issue of privacy has therefore been dispersed into legal categories such as trespass, assault, nuisance, defamation, passing off, infringement of intellectual property rights, and breach of a duty of confidentiality. As causes of action, these were generally adequate for most nineteenth and twentieth century violations of an individual's privacy. The law was concerned to prevent discrete or singular transgressions across the various boundaries that separated the individual from the public world. Such a nineteenth century paradigm, with its bodily and proprietary conceptions, is effectively irrelevant to the digital world, where the threat to the individual arises not from a singular transgression of any discernible boundary but from the anonymous, continuous accumulation of data relating to the individual's digital persona. Moreover, the threat is intensified by the *potential* to merge data bases in which different fragments of information about an individual are located.

The second paradigm, based on monitoring and surveillance, aims to enhance collective security by applying computer technology to the tasks of risk identification and assessment. This represents a departure from traditional criminal law because there is a focus initially on the task of identifying individuals of interest, supported by subsequent endeavours to collect information relating to their connections, associations and patterns of communication. Operations within this surveillance paradigm may even focus on ideas that an individual holds, or is presumed to hold. In all such cases there need be no existing evidence of a crime, or even of an intention to commit a crime. In relation to the Islamic community, this approach is inherently pre-emptive, and is inevitably based on profiling. Considered from this perspective, the paradigm is potentially in conflict with the values of a free and tolerant multicultural society. It certainly appears to sit uneasily alongside concepts of racial discrimination.

In the post-September 11 environment, however, the traditional balance between civil liberties and security has been altered. It now seems that two views of computer ethics sit uneasily alongside each other: on the one hand there is a weak regime of privacy protection in place for ordinary citizens; and on the other hand there is a strong surveillance regime in place for those whom the State regards as a risk to security. Arguably, neither regime is satisfactory: ordinary citizens need more protection from invasive digital technology, and anti-terrorist agencies need more invasive powers so that they can effectively realise the anti-terrorist potential of that same technology**.** Ethically, however, the two regimes are inherently divisive. In place of one law for all, we may be witnessing the emergence of parallel regimes, with each oriented towards a demographic that is defined ex-ante.

The ethical confusions that arise from the existence of these two paradigms reflect the ambivalent potential of the digital revolution. Digital technology poses an enormous threat to individual privacy, yet it also enhances collective security in the so-called war against terror. Individual freedom and collective security, however, are not necessarily antithetical; and nor are democratic rights inconsistent with the existence of a strong State. The question that needs to be asked is this: how can safeguards for ordinary citizens be strengthened, and yet how can the State also have the powers it needs in order to prevent terrorists from achieving their objectives? Before this question can be addressed, other questions need to be answered: who determines if a citizen is or is not an *ordinary* citizen, and when, and by what processes, and by which persons or bodies, is such a determination to be made? Undoubtedly, the post-September 11 world has altered

the perceptions of threat and risk as well as perceptions of the balance that must be struck between liberties and security. Human rights, however, cannot be disregarded or held in suspension, even if the boundaries have shifted and even if the issue is more complex in today's environment than it was hitherto. It is crucial that the two paradigms be kept distinct, and it is crucial that processes be put in place in order to ensure that this is the case. If we are effectively looking at the emergence of parallel systems of law and ethics, then the question is whether Western democracy is sufficiently sophisticated and flexible to accommodate two parallel regimes. There is, of course, one other difficult question: how do we *keep* those regimes separate on an ongoing basis?

A Weak Common Law Conception of Privacy

Although Western individualism evokes a strong sense of privacy, it is hard to disagree with Simitis (1987: 732) when he says that '(f)ar from being considered a constitutive element of a democratic society, privacy appears as a tolerated contradiction'.

The Western tradition of privacy is based on a public/private distinction. Characteristically, we imagine an inner layer or intimate core of the self that retreats from the unwanted intrusion of those people or organisations that operate in the external world (Mitchell 1995: 234). Normally, when we think of an invasion of privacy we have in mind a discrete act that can be categorised as a specific invasion of our intimate or emotional life. In all such cases, there is a discrete act that crosses a boundary. Such an act will generally be perpetrated by a specific person or organisation in a specific instance against a specific physical individual. In this sense, an invasion of privacy is conceptualised as a trespass across boundaries, whether those boundaries are physical, mental or emotional.

Common Law Treatment of Privacy and Individualism: Protection of the Body and Property

The dominance of proprietary conceptions explains the landmark decision in *Victoria Racing Park and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479, when a radio station avoided payment of rights to broadcast by setting itself up outside the ground, but with a clear view of the races that were taking place inside the ground. Importantly, no trespass had taken place. As generally understood, this case was taken to stand for the principle that there was no general right to privacy at common law. It was, of course, a poor set of facts from which to draw such a conclusion. The relationship between the parties was a relationship between impersonal organisations rather than between individuals, and the issue at stake was essentially a commercial one rather than an intimate or emotional aspect of an individual's existence. Rather than privacy, the case turned on the issue of who had proprietary rights to the open spaces of the racecourse and the very public spectacle that took place there. There was little about these facts that was private other than in the proprietary sense of the term.

The more recent Queensland case of *Grosse v Purvis* [2003] QDC 151, however, suggests that the issue is no longer as settled as it recently seemed.

In any event, a concept of privacy based on spatial, bodily, and proprietary metaphors, and on singular or discrete physical acts, is ill-suited to the present-day threats posed by data collection, merged data bases, cookies, web-bugs, cyber tracking and dataveillance. These acts do not involve a trespass as conventionally conceived, and nor do they

constitute an assault, or even a nuisance, as the law currently stands. Whereas conventional conceptions of invasions of privacy evoke a spatial metaphor, or a sense of inner and outer, in a digital environment we are faced with a situation in which there has been a scattering of personal data in a decentred cyber world beyond our sensual experience. Individuals and organisations unknown to us aim to collect and amalgamate otherwise innocuous pieces of data of a more or less public nature, for the purpose of constructing a digital persona. On its own, little of this data would be considered private, at least in the traditional sense of the term. Today, the threat to individual 'privacy' often arises not from any particular act, or from any particular piece of data *per se*, but from the pervasive, constant, cumulative and secretive nature of the process. It is the loss of autonomy that is the threat, and not the invasion of our private or emotional life.

A number of interrelated trends have exacerbated this threat: rapid developments in telecommunications, informatics, biotechnology and genetics have coincided with a convergence of new technologies. The result has been an explosion of sensitive, centralised and cheaply retrieved data that is now stored, not in paper format at separate geographic locations, as was once the case, but in cheaply and easily accessible data bases that can be merged with the click of a mouse (Waters 1997). As Kirby (1998: 5) observes, the technology of the internet 'tends to favour the spread of information' while 'the protection of competing values is weak'

Utilitarian Calculus and the Balance between Western Individual Liberties and the Surveillance Powers of the State

In the nineteenth century, when the liberties of the individual were invoked in order to place limits on the investigative powers of the State, crime was regarded as a marginalised activity undertaken largely by individuals for specific motives — whether they be emotional, sexual or financial —that became manifest in a unique factual context (Weiner 1990). Such motives were readily understood by the general population. In other words, the consequences of any individual criminal acts were regarded as relatively limited in scope, and unlikely to touch the lives of the general population, either individually or *en masse*. Furthermore, weapons were relatively limited in their destructive power, and evidentiary techniques of profiling and surveillance were either unavailable or very expensive, and certainly not generated as a by-product of technological developments in the mainstream economy. In other words, surveillance on a general scale was impossible technically and regarded as undesirable philosophically.

Moreover, crime was not thought to have a significant international element. States did not imagine that there might exist well-organised and well-funded groups or associations of people who acted with a degree of cooperation, autonomy and secrecy in an international setting beyond the control of other sovereign States. All of these considerations meant that, on a utilitarian basis, the protection of civil liberties was accorded a high priority, even if this meant that some people who had committed criminal acts went free. In evidentiary terms, it also meant that a person was not guilty by mere association, or by the thoughts that he or she had. When it came to an attempted crime, the individual had to go some considerable distance in the construction of plans.

September 11 changed all of this. It became quickly apparent that the destructive power of terrorist acts was potentially enormous. It was also clear that non-State terrorist organisations were organised into more or less independent cells.

By its very nature, terrorism is constituted by its links, its connections and its associations. It relies on complex communication and planning, where intent and secrecy go hand in hand. In the age of nuclear and biological weapons, and in the context of very large urban populations, the risks posed by the destructive power of terrorism are immense. The potential crimes or acts are of such magnitude that the calculus underpinning traditional civil liberties has disappeared. States are now thinking in terms of pre-emption and risk management, and this means that they wish to know about personal links and communications between certain individuals as well as what plans they might have. This is the calculus of a surveillance society in which traditional liberties based on ex-poste evidence are in retreat and the new surveillance technology and will of the State, based on ex-ante assessments, are in the ascendancy (Lyon 2001; Lyon 2002).

Perhaps this explains the observations of those such as Robert Warren (2002: 614), who notes the conflation of the public and private and the subjugation of civil society to an increasing militarisation of urban space. Clearly, in the aftermath of September 11 the modern State will seek to use all available technology at its disposal to analyse and evaluate a vast amount of personal data. (Etzioni 2002: 274-80; Hunter 2002). Technologies, political will and administrative capabilities have coalesced at a juncture where it is possible to track cars and mobile phones, and to integrate this data with increasingly sophisticated genetic and biometric data, as well as with data bases developed by various private organisations at different cyber locations.

The problem here is that when any person or organisation is given power, that power must be codified and constrained. The argument that the State should have certain rights might be sound in principle but it is a right that is subject to abuse. Indeed, as Simon Davies (2001) cautions, such arguments feed ‘on hypocrisy, deception and a total absence of any intellectual or analytical foundation, resulting in unreasonable extensions of surveillance’. For this reason it there is a strong argument that the degree of independent external scrutiny should rise in proportion to the concessions that are made in the interests of public safety. This approach would place the burden on government to demonstrate that such concessions are needed. For this purpose, the bar would be set very high (Strossen 2001)

The Issue of Privacy-Enhancing Technologies: Privacy, Encryption and the State

In assessing the role of privacy-enhancing technologies (Arrison 2002) I shall focus on encryption, principally because it brings the underlying issues into sharpest focus. In the post-September 11 environment some American observers see cryptographers as existential heroes in a new techno-frontier, defeating the malevolent and conspiratorial impulses of national government. Westin (1998), for example, in his keynote address to a 1998 conference on Privacy and the Internet, invoked Western frontier imagery when he said: 'As in the earliest days in America, the Internet abounds with modern day cattlemen, sheep-herders, farmers, saloon keepers, whores, and hacker-gunmen, with the influences of the schoolmarm, minister, sheriff, and judge also struggling to be heard and felt'. Mike Godwin (2003:158) suggests that 'at a deep level, the philosophical issues raised by cryptography...centre on the question of whether we believe that human beings, once empowered to speak anonymously and secretly, are more likely to use their new powers unjustly, to do harm to others, than to act with integrity'.

In the post-September 11 world (Graham 2002; Lyon 2003), can such a utopian ontology of the human subject really be the basis for legal and ethical thinking about the issue of data security in a global environment of transnational terrorist cells?

Godwin can only conduct his argument along these lines by fixating on one principle and ignoring all other competing principles, such as risk identification and management. The management of risk, however, is not antithetical to the defence of civil liberties, and nor is a strong State antithetical to the preservation of either individual freedoms or individual autonomy. Only a strong State is capable of preserving the processes and procedures, the checks and balances, and the dispersal of decentred governmental and corporate power that are essential for the preservation of privacy and individual rights.

Does the State have a reasonable and legitimate interest in searching an individual's private location in cyberspace, just as it has an interest in searching inside real private spaces, such as houses and workplaces? Such a right in the physical world is commonly accepted, so long as it is subject to proper legal process. The issue at hand here is whether the processes and protocols of real space apply, or can be reasoned by analogy to apply, in the digital world. Some writers, such as William Mitchell (1995), structure their arguments by using precisely this kind of analogy. Mitchell, for example, says that '(i)n physically constructed cities, the enclosing surfaces of constituent spaces — walls, floors, ceilings and roofs — provide not only shelter, but also privacy'(at 234). Mitchell argues that access to such spaces are controlled by specific mechanisms: you can lock your doors or leave them open, lower the window shades or raise them'. He suggests that '(s)patial divisions and access control devices are deployed to arrange spaces into hierarchies grading from completely public to utterly private'(at 234).

Drawing on a more traditional and emotive concept of intimate privacy, Mitchell sees the Western house as a metaphorical model for the cryptographic architecture of cyber space. In the Western house, he observes, 'there is a carefully organised gradation from relatively public verandahs, entry halls, living rooms and parlours to more private, enclosed bedrooms and bathrooms where you can shut and lock the doors and draw the shades against the outside world'. He argues that in virtual cities 'construction technology...must provide for putting up boundaries and erecting access controls, and it must allow cyberspace architects...to organise virtual places into public-to-private hierarchies' (at 235). According to Mitchell, 'the rough equivalent' of a locked door or gate is an authentication system, where a password and identification system functions like a set of keys. Passwords, however, are analogous to keys in another regard: they can be stolen or copied. They therefore merely discourage illicit entry, but will not block the determined thief. The 'strongest of enclosures around digital information' (at 235) is provided by encryption, whereby the information is scrambled in a complex manner so that it can only be decoded by somebody in possession of a correct and secret numerical key. Each user would have both a public key and a secret private key. The sender would first obtain the recipient's public key, and use that to encode the information. The recipient would then decode it using the private key.

These suggestions, however, raise a number of questions. Can methods of dealing with privacy and data security be left simply to the private decisions of individuals and to the future patterns of development in the field of digital architecture? Can questions of morality and ethics be pushed to one side as this complex issue is resolved in the course of a techno-battle, where surveillance technologies and their cryptographic counterparts

are ushered onto the cyber battlefield with a click of the mouse? Isn't this simply techno-anarchy? Can we really link cryptography with liberty and privacy, and the impulse to impose legislative controls with the sinister objectives of a malevolent Orwellian State? Alternatively, can't it be argued that democratic freedoms are enhanced by a strong State that is subject to the principles of transparency and accountability?

Cryptography should not be seen in essentialist terms, as though it naturally and automatically enhances the value of privacy. There is always a human context to the use of technology. In certain circumstances encryption can be used to perpetrate the most serious violations of individual privacy. The Privacy and Innovation Unit Report on encryption provided to the UK Government in 1999 highlights some key examples of such violations in the area of child pornography, where encrypted images were sent to contacts around the world (1999: 7).

The problem with powerful encryption, as Etzioni (2002: 265) observes, is that 'it is qualitatively different from the impact of other privacy-enhancing technologies'. He argues that in the past the main factor that constrained public authorities when new technologies emerged was the obsolescence of existing laws. In the case of strong encryption, however, 'the technology imposes its own barrier'. The problem can no longer be solved by updating the law. Public authorities now understand that 'no court order can enable strong encryption to be broken' (Etzioni 2002: 265).

Cryptography undoubtedly makes an important contribution to internet security, and there is a strong case for its universal availability, but there is also a strong argument that it should be subject to the checks, controls and due processes of civil society. Etzioni is surely right when he says that 'it is difficult to sustain the argument that the government should be unable to decrypt any messages or be unable to gain the authority to do so' (Etzioni 2002: 281-82). The most important objectives are to determine which messages can be decrypted; under what circumstances and by what processes permission to do is to be granted; who is to verify that independently determined limits have been observed; and by what means such verification will be undertaken.

The need to address these issues is urgent. Denning (1996) suggests that 'the widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception (wiretaps) and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight'. She argues that the consequences would be 'devastating'. In her view, computers and telecommunications systems would be 'become safe havens for criminal activity' of various kinds: tax evasion, money laundering, industrial espionage, the purchase and sale of electronic information on black networks, the corruption of corporate records, and the rendering of corporate and other information inaccessible.

Denning suggests that 'by strengthening the integrity of evidence and binding it to its source, cryptographic tools for authentication are a forensic aid to criminal investigations'.

In a democracy, the desirable principle is that power should be divided and then dispersed in such a way that it is subject to discussion, review and even contestation. Negotiation and due legal processes ideally exist wherever power is present.

One option is to develop legislation designed to encourage the wide use of trusted third parties. This would have the effect of maintaining data security, privacy and

confidentiality under normal circumstances while providing for a dispersal and fragmentation of power. There is also one other benefit: as Greenleaf (1996) suggests, third parties are easier to serve with warrants while maintaining covert operations. If Trusted Third Parties are licensed, then law enforcement agencies are able to pursue serious crime by establishing procedures by which encryption keys would be disclosed to them. These procedures would have safeguards similar to those that already exist with respect to telecommunications legislation.

CONCLUSION

The Australian legislation is notable not for its strict protection of privacy, but for the large number of exemptions it allows. In this context, Davies (2001:7) is surely correct when he argues that '(t)he preservation of privacy should not be viewed as an encumbrance that can be diluted through 'public interest' exemptions, but as a public interest *in itself*'.

Given that the scope and ambition of the legislation is restricted, it is difficult to see the Australian response as anything other than a dismal failure in terms of both its objectives and its outcomes. The Australian legislation could be seen as a cynical perversion of a fair practices movement that itself is already deeply flawed. Indeed, the legislation may have a pernicious consequence to the extent that it diffuses the issue and provides a false sense of security to those who think that legislative controls have been put in place.

This confused and inadequate regime now sits vaguely and uneasily alongside a rapidly emerging surveillance regime based on risk management, profiling and pre-emption. Before we, as a society, can begin to deal with the potential consequences of these developments, we need to articulate the ethical issues that arise.

The Australian legislation is notable not for its strict protection of privacy, but for the large number of exemptions it allows. In this context, Davies (2001:7) is surely correct when he argues that '(t)he preservation of privacy should not be viewed as an encumbrance that can be diluted through 'public interest' exemptions, but as a public interest *in itself*'.

Given that the scope and ambition of the legislation is restricted, it is difficult to see the Australian response as anything other than a dismal failure in terms of both its objectives and its outcomes. The Australian legislation could be seen as a cynical perversion of a fair practices movement that itself is already deeply flawed. Indeed, the legislation may have a pernicious consequence to the extent that it diffuses the issue and provides a false sense of security to those who think that legislative controls have been put in place.

This confused and inadequate regime now sits vaguely and uneasily alongside a rapidly emerging surveillance regime based on risk management, profiling and pre-emption. Before the policy issues and the consequences of these parallel streams can be addressed, the ethical issues will have to be given more thought than they have so far received.

REFERENCES

Cases

Grosse v Purvis [2003] QDC 151

Victoria Racing Park and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479.

Statutes

Privacy Act (Cth) 1988
Privacy Amendment (Private Sector) Act (Cth) 2000
Information Privacy Act (Vic) 2000
Workplace Video Surveillance Act 1998 (NSW)
Surveillance Devices Act 1999 (Vic)

Other References

Armstrong, Paul and Cox, Brian, (2001), Privacy, Health Information and Employee Records: Implications of New Commonwealth Privacy Laws, paper presented at *PACRIM2001*, Cairns, 9 October 2001, accessed at http://www.privacy.gov.au/news/speeches/sp60note.html

Arrison, Sonia, (Feb 2002), "How You Can Protect Your Privacy, Consumers' Research Magazine', Vol. 85, no. 2,), 10, accessed at *<http://0=proquest.umi.com.alpha2.latrobe.edu.au/pqdweb?index=42&sid=3&srchmode=1&...>*.

Australian Law Reform Commission (ALRC) and The Australian Health Ethics Committee (AHEC). (2003). *Essentially Yours: The Protection of Human Genetic Information in Australia,* May [2003}.

Borking, John (2000), 'Privacy Incorporated Software Agents: A Proposal for Building a Privacy Guardian for the Electronic Age', *PLPR* 46,

Bygrave, Lee (2001), 'The Place of Privacy in Data Protection Law', *UNSWLJ* 6, accessed at <*http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6html*>.

accessed at <*http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/2000/46.html?query=28%*>.

Bygrave, Lee A.(2001). A right to privacy for corporations? Lenah in an international context, *Privacy Law and Policy Reporter*, pp. 130-134.

Clarke, Roger (2001a). Privacy as a Means of Engendering Trust in Cyberspace Commerce, *UNSWLJ* 8, accessed at < *http://www.austlii.edu.au/au/journals/UNSWLJ/2001/8.htmL>l*.

Clarke, Roger (2001b). Person-Location and Person-Tracking Technologies: Technologies, Risks and Policy Implications, accessed at <*http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html*> 2001.

Clarke, Roger (2004). Resources: Workplace Privacy, Version of 20 September 1999 (plus revisions to Sep 2004), at *http://www.anu.edu.au/people/Roger.Clarke/DV/Workplace.html*

Davies, Simon (2001). Unprincipled Privacy: Why the Foundations of Data Protection are Failing Us, *UNSWLJ 7*, accessed at <*http://www.austlii.edu.au/au/journals/UNSWLJ/2001/7.html*>.

Denning, Dorothy E [1996], 'The Future of Cryptography', PLPR, 26, accessed at *http://www.austlii.edu.au/cgi-bin/disp.pl/au/joUrnals/PLPR/1996/26.html?query=encrypt%2a*

Electronic Frontiers Australia (2000). *Submission to House of Representatives Standing Committee on Legal and Constitutional Affairs: Inquiry into Privacy*

Amendment (Private Sector) Bill 2000, May 2000. accessed at <*http:www.efa.org.au/Publish/privacy_inquiry_2000.htm*>.
Electronic Privacy Information Center (2004). *Workplace Privacy*, accessed at http://www.epic.org/privacy/workplace/
Etzioni, Amitai (2002), 'Implications of Select New Technologies for Individual Rights and Public Safety', 15 *Harvard Journal of Law and Technology* 257.
Godwin, Mike (2003), *Cyber Rights: Defending Free Speech in the Digital Age*, Revised and Updated Edition, MIT Press, Cambridge , Massachusetts.
Graham, Stephen (2002), 'Special Collection: Reflections on Cities, September 11th and the 'War on Terrorism' - One Year On', *International Journal of Urban and Regional Research*, 26(3), 589-590.
Greenleaf, Graham[1996], 'The Scramble to Develop Encryption Rules', *PLPR* 35, accessed at *http://www.austlii.edu.au/cgi-bib/disp.pl/au/journals/PLPR/1996/35.html/query=encrypt%2a*
Hunter, Richard (2002), *World Without Secrets: Business, Crime and Privacy in the Age of Ubiquitous Computing*, Wiley, London.
Kirby, Justice Michael (1998). Privacy and Cyberspace, *UNSWLJ 46*, accessed at <*http://www.austlii.edu.au/au/journals/UNSWLJ/1998/47/html*>.
Lyon, David, (2001) *Surveillance Society*, Open University Press, Buckingham.
Lyon, David (ed) (2002) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, Routledge, London.
Lyon, David (2003), *Surveillance After September 11th*, Basil Blackwell, Oxford.
Mitchell, William (1995). Soft Cities, in *City of Bits: Space, Place and the Infobahn*, accessed in (ed) Neil Spiller , *Cyber_Reader: Critical Writings for the Digital Era*, Phaidon, London, 2002.
NSW Ombudsman (2004). *Submission to the review of the Privacy and Personal Information Protection Act 1998, Annexure A: A New Approach to Privacy Regulations*.
Office of the Federal Privacy Commisioner (OFPC), *Guidelines on Workplace Email, Web Browsing and Privacy*, accessed at <*www.privacy.gov.au*>.
UK Cabinet Office (1999), *Encryption and Law Enforcement*, A Performance and Innovation Unit Report.
Rodota, S (1976). Privacy and Data Surveillance : Growing Public Concern, *OECD Information Studies10: Policy Issues in Data Protection and Privacy*, OECD, Paris.
Simitis, Spiros (1987). Reviewing Privacy in an Information Society, *University of Pennsylvania Law Review*, 135 707.
Strossen, Nadine, (Nov. 26, 2001), 'Remarks at the Communitarian Dialogue on Privacy v Public Safety', accessed at <*http://www.gwu.edu/ccps/privtrans.html*>.
Warren, Robert (2002), 'Situating the City and September 11th: Military Urban Doctrine, 'Pop Up' Armies and Spatial Chess', *International Journal of Urban and Regional Research*, 26(3), 2002, 614-619, at 614.
Waters, Nigel (1997) Telecommunications: the Privacy Frontline, *PLPR* 56, accessed at <*http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1997/56.html?query=%28...*>.

Weiner, Martin J (1990) *Reconstructing the Criminal: Culture, Law, and Policy in England, 1830-1914*, Cambridge, Cambridge University Press.
Westin, Alan F (1998) *Privacy on the Internet: Everyone a Data Protection Officer?*, Keynote Presentation, accessed at <*hhhtp://www.privacyexchange.org/iss/confpro/westinkeynote.html*>

Computer simulations, disclosure and duty of care

John Barlow
Australian Catholic University
Sydney, Australia.

Abstract

Computer simulations provide cost effective methods for manipulating and modeling 'reality'. However they are not real, they are imitations of a system or event, real or fabricated, and as such mimic, duplicate or represent that system or event. The degree to which a computer simulation actually aligns with and reproduces the 'reality' of the system or event it is attempting to mimic or duplicate is dependent upon many factors, including for example, the efficiency of the simulation algorithm, the processing power of the computer hardware used to run the simulation model, and the expertise, assumptions and prejudices of those concerned with designing, implementing and interpreting the simulation output. Computer simulations in particular are increasingly replacing physical experimentation in many disciplines, and as a consequence, are used to underpin quite significant decision-making which may in many instances impact on 'innocent' third parties. In this context then, this paper examines two interrelated issues: Firstly, how much and what kind of information should a simulation builder be required to disclose to potential users of the simulation? Secondly what are the implications, if any, for a decision-maker who acts on the basis of their interpretation of a simulation output without any reference to its veracity, which in turn comprises the safety of other parties?

Keywords: Modeling and simulation, ethics, disclosure, duty of care, responsibility.

INTRODUCTION

In general terms a model may be described as a possible representation of the connected variables, or conditions, that are assumed to be operating within a system or an event while a simulation may be described as an attempted reproduction, using a model, of the conditions that define a system or event. Computer-based simulations may, at one level, involve the use of 'unsophisticated' spreadsheet and database applications to simulate and predict events that can, in the main, be conveniently modelled using mathematical relationships. For many people however, a computer-based model or simulation often means a multimedia application, such as a virtual reality application which provides them with the opportunity to 'experience' various situations, using the computational power of modern computer platforms, and their associated user and graphical interfaces, to generate interactive images of ‘very real’ situations.

Numerous authors have provided definitions of computer-based modeling and simulation, together with descriptions of where they are used in various human activities. Essentially there are a number of themes that run through the definitions, the most notable of which is the notion that simulations provide cost effective methods for manipulating and modeling 'reality'. There are many instances that illustrate this view. For example, architectural design simulations, which permit prospective buyers to walk through a new home design, are now frequently used as marketing tools. Metallurgists are cautiously hopeful that the combination of more sophisticated simulation algorithms combined with increased computer processing power will further enhance their understanding of crack propagation in metals. In reality, computer-based simulations are utilised in just about every human endeavour including playing games for pleasure and entertainment, modeling courtroom evidence and complex experimental data, graphing philosophical paradoxes, and providing sophisticated modeling mechanisms for predicting the weather! In addition simulations are used in many application areas, most notably defence applications where, for example, military scenarios can be modelled and evaluated without the need to subject military personnel to real and potentially hazardous combat conditions.

Shelly, Cashman & Vermaat (2002, p. 6.43), suggest computer simulations are *computer-based models of real-life situations*. Computer applications of models and simulations are used to support computer-aided decision-making associated with such activities as design, testing, planning, and control. Ören (2000, p. 166) suggests simulation can be defined as *goal-driven experimentation with dynamic models*. He argues that the reasons for using simulation vary with the type of area of study and briefly sets out a number of examples. These include analysis problems where simulation is used to provide insight, continuous simulation used as part of the design process (particularly in engineering design), and discrete simulation used in association with business applications. Other instances include artificial intelligence applications used in simulation software, autonomous software agents, Internet simulations using local, or network computational platforms, as well as defence applications as noted above.

Singh (1996, pp. 560-561), has adopted the combined term, 'simulation model', and defines it as a *concise framework for the analysis and understanding of a system* that *facilitates imitating the behaviour of the system over time*. He asserts that simulation-modeling techniques are powerful and cost effective tools for manipulating time, system inputs, and the logic combinations associated with complex systems. Moreover, when combined with visual animation equipment simulation modeling techniques provide an efficient means of learning about, experimenting with, and analysing real-life complex systems.

One of the important considerations of Singh's definition relates to the observation that simulation is synonymous with imitation, and while his work is strictly focused in the context of complex computer integrated manufacturing and design systems, they have merit in the wider context of computer modeling and simulation. It is an important observation in that it underlines the important, if not cautionary point that computer simulations are not real, they are imitations of a system or event, real or fabricated, and as such mimic, duplicate or represent that system or event. The degree to which a computer simulation actually aligns with and reproduces the 'reality' of the system or event it is attempting to mimic or duplicate is dependent upon many factors. These factors include, but are not limited to, the efficiency of the simulation algorithms, the processing power of the computer hardware used to run the simulation model, and the expertise, assumptions and prejudices of those concerned with designing and implementing the models and simulations.

Codes of professional ethics and professional practice

In the general sense, codes of professional ethics and professional practice of various organisations provide a set of guidelines for the conduct of their members. The two codes are notionally differentiated by their intent. Codes of ethics are intended to provide fundamental guidance, which should permeate the conduct of an organisation's member, while the code of practice is designed to provide more specific guidelines regarding acceptable standards of professional practice. Essentially the development and adoption of codes of ethics and practice by organised groups reflect their desire, in part, to be seen and accepted as 'professional' entities in the wider community, and their member's as 'experts' in their chosen field.

The expanding importance and scope of the various application areas of modelling and simulation has prompted the call for the establishment of a professional code of ethics for those involved in the development of computer-based simulations. Mulvey (1994, p. 54) argued in the context of computer modeling that since the actions of modelers can impact on others "*codes of ethical conduct represent attempts to reduce harm when professionals carry out their business*". This view is supported by Ören (2002a) who has suggested that, given the expanding importance of their work, simulators are now *obliged* to reflect on the professional and ethical implications of their work. Ören (2002b) has asserted that a code of professional ethics should be formulated and adopted for simulators since ethics was the missing link [between] serious validation as well as verification studies of modelling and simulation. He argued that since simulation studies could affect numerous people as well as the environment in many different ways, those

involved in any aspect of it should reflect upon their responsibilities. Further, simulations are used in many disciplines, such as research, scientific and engineering applications, and business, where specific codes of professional ethics and practice already exist and as such simulators should, at the very least, be aware of such codes. He also suggested that various simulation societies should provide leadership in urging their members to adopt a code of professional ethics so that their members "*can show the acceptance of their responsibilities and accountabilities*."

A Code of Professional Ethics for Simulationists (SimEthics) has since been established by the Society for Modeling and Simulation International. This is a voluntary code and is no doubt an important development given the nature of the interaction between computers, simulators, computer applications, and the general public. Ferguson (1992) [quoted by Beder (1998, p. 49)], for example, asserts that commercial software programs are becoming increasingly available for all sorts of design problems. These programs, argues Ferguson, offer 'illusions of certainty' without reducing the need for human judgment requiring 'intimate, first hand internalized knowledge' of the technology being used and the impact that this might have on product outcomes, a view supported by Girill (2002).
The real issue of course in this instance is how such codes can be implemented and used to guide the professional practice of simulators. One issue worth exploring in this context is the need for the disclosure of information about a simulation and the associated duty of care implications.

Disclosure and duty of care

The need for the disclosure of information associated with simulations is an emerging issue. That is, how much information should a simulator be compelled to inform their colleagues and potential users, both from within the professional and public domains, about the limitations and assumptions underpinning the development of a simulation? The quality of a simulation is very much dependent upon the quality of the model it has been developed from, which implies of course that it is fundamentally dependent upon the quality of the data used to develop the model. In addition, there is also an argument relating to the right, or perhaps even more importantly responsibility, of a simulation user to know what the simulation package is actually designed to model, and how it should be interpreted. This should include information about the context, circumstances, and design constraints associated with the development of the model, the range and type of testing data used to verify the validity and reliability of the simulation, as well as information indicating the intended applications of the simulation.

Girill (1999), for example, has noted, "*software trends already underway make computer documentation the next major venue for the appropriate disclosure of relevant facts that once might have remained hidden*." He observed that sophisticated computer simulations in particular are increasingly replacing physical experimentation in many disciplines, such as engineering and medicine, and as a consequence are used to underpin quite significant decision-making. In essence the decision-maker is increasingly vulnerable to the quality and appropriateness of the assumptions the software programmer has made when developing the simulation. Girill (1999) makes an important point when he asserts:

> "Disclosing hidden software assumptions, and spelling out their implications for the output of simulation runs, will have a major impact on how astutely engineers and physicians can make good judgements based on simulated, rather than physical analysis."

Users, and in particular uncritical users and third parties such as members of the 'public' not directly involved in the building, implementation and interpretation of models and simulations, are very much dependent upon the competence and professional expertise of simulation builders and users. These individuals would probably have not seen it necessary, or perhaps not even been aware that they should have, carried out some form of risk assessment in relation to the model, the simulation, the output, and the interpretation of the output by 'experts'. They are thus forced into a trust relationship between themselves and the expert simulation builders and users, implying that they believe them to be honest and true, which also significantly implies a degree of dependency and vulnerability. This point has been noted by Fullinwider, (1995, p.2) as one of three that distinguishes a profession, the other two being an orientation to public good, and a specialized knowledge and training, and has clear duty of care implications.

In general, a duty of care requires all individuals to do what is reasonable to protect the wellbeing of others. For example, a legal duty of care is placed on all employers, their employees and any others, including contractors, to do everything reasonably practicable to protect the health and safety of all individuals from hazards in a workplace. A professional duty of care also involves harm minimization, acting in a client's best interest and exercising discretionary power responsibly. In particular, Ören (2002a), for example, has suggested that the major components of professionalism in modelling and simulation are knowledge, activities, and behaviour. That is, according to Ören (2002a), "*knowledge is essential to perform the activities which in turn should be based on acceptable behaviour"*.

Manufacturers and suppliers of consumable goods have a duty to provide products that do not compromise the safety of consumers. Indeed, legislation imposes statutory warranties of fitness for purpose which are contractually binding between seller and purchaser. The use of any product though involves an inherent degree of risk. Heckman and Wobbrock (1998, p. 394) assert:

> "Strict products liability recognizes that with modern technology and mass production, injuries will occur without intentional misdeed and despite reasonable care."

By implication then individuals and organizations that provide computer models and simulations, also have a duty to provide products that maintain the safety and wellbeing of others. That said, the nature of the risks can vary significantly over a wide range of issues, including for example, an inherently defective product produced without reference to new methods and standards, misinterpretation of output, or inappropriate use occasioned by the provision of poor, inappropriate or no training of users. Like other

products, faulty simulation products can result in negligence actions. There are various legal options available for defending charges of negligence, and in relation to computer usage in particular there appears to be no clear standards (Nissenbaum, 1994, 1996). However this should be no excuse. It would seem reasonable to argue that all builders and users of computer simulations, and in particular those who would identify themselves as experts and members of a professional body, should exercise as an inherent code of practice, a moral responsibility for their products.

Weckert & Adeney (1997, p. 89) argue that "experts have a responsibility to be careful, competent, and honest in their work" and that the word "responsible" has two important senses: causal (cause and effect) and accountability (liability). Hart (1985) [quoted by Coleman (2005)] has suggested a broader interpretation of responsibility identifying four senses. These are:

- Role-responsibility (the performance or fulfillment of the duties attached to a person's social role),
- Causal-responsibility (a retrospective sense of responsibility relating cause and effect between a person's actions and the consequences of them),
- Liability-responsibility (responsibility for causing harm in violation of the law), and
- Capacity-responsibility (the capacity to understand the conduct required by relevant societal norms, and then to act appropriately).

Coleman (2005) writing in the context of computer systems generally has suggested these senses 'provide a framework for exploring computers and moral responsibility'. These include: a retrospective analysis of 'who is responsible for computer use', the anticipation and prevention of future problems, a consideration of whether computers could be responsible, and an assessment of the decisions computers should not be allowed to make.
She also provides a very useful analysis of the difficulties associated with identifying who are the responsible parties in relation to computer use, which centres on four barriers to responsibility identified by Nissenbaum (1994, 1996):

- The problem of many hands,
- Bugs,
- Blaming the computer, and
- Ownership without liability, as well as two others:
- Poor articulation of norms, and
- Assumption of ethical neutrality.

A summary of Coleman's analysis is set out in table 1.

Barrier	**Description**	_Problem of many hands	Complex computer	_Bugs' and 'computer	'Bugging the computer is	_Blaming computer is	A common ofte	_Ownership without	Extending the	_Poor articulation of	A poor understandi	_Assumption of ethical	Problem and solution

han ds	syst ems are pro duc ed by gro ups mak ing it diffi cult to iden tify who is resp onsi ble for erro rs and har mfu l con seq uen ces of use.	erro r’ are pref erre d to ‘pro gra mm er erro r’ disc oura ging hum ans fro m inte rpre ting thes e erro rs as thei r own (Go tter ban, 200 1).	the pro xim ate caus e of har m. Peo ple ofte n attri bute inte ntio nalit y to com pute rs. Peo ple hav e ‘del egat ed’ or ‘abd icat ed’ thei r deci sion mak ing to com pute rs (La dd, 198 9, p. 219). Peo ple hav e high exp ecta tion	liabies and righ ts of own ersh ip of soft war e syst ems with out dem andi ng own ers acce pt resp onsi bilit y for thei r pro duct s (Nis sen bau m, 199 4, 199 6).	nor ms	ng of wha t eac h part y in the crea tion , imp lem enta tion , and use of a syst em is resp onsi ble for doin g (Joh nso n & Mul vey, 199 5).	neut ralit y	s are artic ulat ed and dev elop ed in a cont ext in whi ch thei r imp act on hum anit y is less visi ble than it sho uld be (Go tter ban, 200 1).

s of com pute rs (Joh nso n & Mul vey, 199 5). Onc e com pute rs are bla med ther e is no nee d to inve stig ate othe r hum an fact ors.

Table 1: Responsibility barriers

Discussion

Clearly disclosure and duty of care are complex matters. For example, not only how much and what type of information should be disclosed is important, but also to whom should it be reasonably disclosed (colleagues, independent referees, members of the public)? In addition issues associated with intellectual property, the copyright and patenting of new simulation systems, and the possibility of industrial and international espionage especially given the increasing reliance of the defence sector on the use of computer-based simulations are also worthy of attention.

A further issue related to disclosure and candour centres on the substance of the detail contained in the information to be released. Even partial disclosure of the rationale underlying a model might result in an increase in the authority and mystique associated with the use of and results generated by the simulation which are totally unwarranted and which may lead to unintended harm. Disclosure may provide a simulation with a 'credibility aura' well beyond its actual merits, particularly in the public domain where knowledge of the mathematical assumptions and other theories underpinning the simulation design and implementation is either non-existent or perhaps little understood. It may also result in the reverse.

Sterman (1991, p.209), for example, observes that most people are not able to make judgments about the veracity of computer models in an intelligent and informed manner, and makes the point that computer models can be misused, accidentally or intentionally.

> "Thus there have been many cases in which computer models have been used to justify decisions already taken, to provide a scapegoat when a forecast turned out wrong, or to lend specious authority to an argument."

A basic consideration here is who is ultimately accountable in these circumstances if a decision made on the basis of a simulation results in harm to an individual or group either directly or indirectly? Where does the duty of care lie? Weckert & Adeney (1997, p. 91) have set out three conditions for establishing accountability. These can be interpreted as: control, intention, and free choice. It would seem reasonably obvious then that the misuse of computer simulations might hold the individuals concerned liable to account for their actions, assuming of course that they have not been coerced. This is an important consideration given the often quite deliberate, or otherwise, assertions of 'experts' reporting the results of their work, or politicians and government spokespeople explaining a controversial public policy matter, quite often emphasizing the use of computer modeling and simulations to substantiate and support their assertions and arguments. This may directly or indirectly provide their assertions and arguments with a degree of implied authenticity and authority. There is a possible argument for suggesting that uncritical public trust or confidence in the authority of an expert who suggests, directly or even indirectly, they are using a computer model to support and validate an argument or observation might be somewhat naive and misplaced. Perhaps the question is really this: Is it the implied or actual use of the computer, or the model and simulation, or both, which assigns credibility to the expert advice? The simple reality is, as already

noted above, the quality of the output generated by a computer-based model or simulation is critically dependent on the quality of the data used and the manner in which it was designed and implemented, not necessarily because it was modeled in a computer, even allowing for the fact that modern super computers undoubtedly provide the means for very sophisticated and rigorous modeling and simulations in real time.

Sterman (1991, p. 209) has argued that whether members of society like it or not they are all becoming consumers of computer models. Importantly he observed:

> "The ability to understand and evaluate computer models is fast becoming a prerequisite for the policymaker, legislator, lobbyist, and citizen alike."

That is, all members of society will need, to some extent, be prepared to accept the responsibility of carrying out some form of appropriate due diligence. In order for this to occur though, a supportive and perhaps even enforceable structure needs to be developed. One way forward here might be the consideration of a 'boundaries of responsibility' concept. This could be based on agreed need to know (or entitlement to know) protocols, which set out the type of information that should be reasonably disclosed, by whom and to whom, at each simulation design and implementation stage. A possible research focus might involve the development and implementation of a set of information 'boundaries' which outline the rights, entitlements, and responsibilities of simulators and various application users and consumers (including the public domain), so that all concerned are afforded the opportunity to make reasoned, independent and critical decisions about the merits, or otherwise, of the output and use of computer-based simulations. Clearly this may have significant professional practice implications for simulators, as well as those who use simulation 'tools' as part of their daily responsibilities, be they employment based or otherwise. At a basic level, the 'boundaries of responsibility' proposal looks very much like another code of practice, and might well be so. However it does suggest the incorporation of groups beyond the simulation profession, such as simulation users and public consumers, who also make decisions, both directly and indirectly, based on the work of simulators. Coleman (2005) has provided three recommendations for overcoming the series of barriers to responsibility noted earlier which may help to support and regularize this process. These are:

- Ensuring understanding of (and assumptions about) responsibility is appropriate for the task by using the practice of responsibility to improve both practice and technology.
- Re-designing computer systems to reveal that they are not responsible.
- Articulating those norms most relevant to the creation, implementation, and use of computer systems.

One final point. Mistakes can and do occur. Coyle (1977) [quoted by Coyle and Exelby (2000, p.32)] states 'there are almost endless opportunities for making mistakes in any kind of model building', but as Heckman & Wobbrock (1998, p.399) have asserted:

> "Humans should be responsible for the actions of their creations."

Notwithstanding they were writing specifically in the context of autonomous agents, their assertion is relevant to the moral and professional responsibilities the wider modeling and simulation community should be prepared to accept.

CONCLUSION

In the context of professional practice, the need for disclosure and duty of care were examined as matters which needed further consideration in the development and implementation of computer models and simulations. It was suggested that all simulation builders and users should be prepared to exercise an inherent moral responsibility for their work.

REFERENCES

_____ 1995, Duty of Care, *Industry Commission, Work, Health and Safety*, Report No. 47, Sept., (http://www.nohsc.gov.au/OHSLegalObligations/DutyofCare?dutycare.htm accessed 22 July 2005)

Andradóttir, S., Healy, K. J., Withers, D. H. & Nelson, B. L. (eds) 1997, *Proceedings of the 1997 Winter Simulation Conference*

Barney, G. O., Kreutzer, W. B. & Garrett, M. J. (eds) 1991, *Managing a Nation The Microcomputer Software Catalog* 2nd ed, Westview Press, Boulder.

Beder, S. 1998, *The New Engineer. Management and Professional Responsibility in a Changing World,* Macmillan, South Yarra.

Coleman, K. G. 2005, Computing and Moral Resonsibility, *The Standford Encyclopedia of Philosophy (Spring edition),* Edward N. Zalta (ed). (http://plato.stanford.edu/archives/spr2005/entries/computing-responsibility accessed 10 August, 2005)

Coyle, R. G. 1977, *Management Systems Dynamics*, Wiley, Chichester, in Coyle, G. & Exelby, D. 2000.

Coyle, G. & Exelby, D. 2000, The validation of commercial system dynamics models, *System Dynamics Review*, Vol. 16, No. 1 (Spring), pp27-41.

Fullinwider, R. 1995, Professional codes and moral understanding, *Res Publica*, 4, pp. 1-6.

Girill, T. R. 1999, The Duty of Candor in Future Software Documentation, *46th Annual STC Conference*, Cincinnati, Ohio. (http://www.stc.org/46thConf/postconf/girill.html, accessed 4 November, 2003)

Gotterbarn, D. 1995, The Moral Responsibility of Software Developers: Three Levels of Software Engineering, *Journal of Information Ethics*, Vol. 4, No. 1, pp. 54-64., in Coleman, K. G. 2005.

Hart, H. L. A. 1985, Punishment and Responsibility, in Coleman, K. G. 2005.

Heckman, C. & Wobbrock, J. O. 1998, Liability for Autonomous Agents, *Autonomous Agents '98*, pp392-399.

Johnson, D. G. & Mulvey, J. M. 1995, Accountability and Computer Decision Systems, Communications of the ACM, Vol. 38, No. 12, pp. 58-64.

Ladd, J. 1989, Computers and Moral Responsibility, in *The Information Web: Ethical and Social Implications of Computer Networking*, Gould, C. (ed), Westport Press, Boulder, in Coleman, K. G. 2005.

Mulvey, J. M. 1994, *Models in the Public Sector: Success, Failure and Ethical Behavior*, in Wallace, W. A. (ed), pp 58 - 73.

Nissenbaum, H. 1994, Computing and Accountability, *Communications of the ACM*, Vol. 37, No. 1, pp. 73-80, in Coleman, K. G. 2005.

Nissenbaum, H. 1996, Accountability in a Computerized Society, Science and Engineering Ethics, Vol. 2, pp. 25-42 in Coleman, K. G. 2005.

Ören, T. I. 2000, Responsibility, Ethics, and Simulation*, TRANSACTIONS of The Society for Computer Simulation International*, 17, 4, pp165-170.

Ören, T. I. 2002a, Growing Importance of Modeling and Simulation*: Professional and Ethical Implications, in Proceedings of the ICSC'2002 – The 5th Conference on System Simulation and Scientific Computing*.

Ören, T. I. 2002b, Rationale for a Code of Professional Ethics for Simulationists, *Proceedings of the Summer Computer Simulation Conference*.

Rogers, R. V. 1997, What makes a modeling and simulation professional?: The consensus view from one workshop, in Andradóttir, S. et al (eds) *Proceedings of the 1997 Winter Simulation Conference*, pp1375-1382.

Shelly, G. B, Cashman, T. J. & Vermaat, M. E. 2002*, Discovering Computers 2003 Concepts for a Digital World*, Thompson Course Technology, Boston, MA.

Singh, N. 1996, *Systems Approach to Computer-Integrated Design and Manufacture*, John Wiley & Sons, New York.

Society for Modeling and Simulation International 2005, *A Code of Professional Ethics for Simulationists (SimEthics)*, http://www.site.uottawa.ca/~oren/SCS_Ethics/ethics.htm).

Sterman, J. D. 1991. *A Skeptic's Guide to Computer Models*, in Barney, G. O., Kreutzer, W. B. & Garrett, M. J. (eds) 1991, pp. 209-229.

Wallace, W. A. (ed) 1994, *Ethics in Modeling*, Elsevier Science, Oxford.

Weckert, J. & Adeney, D. 1997*, Computer and Information Ethics*, Greenwood Press, Westport.

COPYRIGHT

A Taxonomy of Penetration Testing Ethics

Justin D. Pierce[1], Ashley G. Jones[2] and Matthew J. Warren[1]

1: School of Information Systems
Deakin University
Victoria, Australia
jdpierce@deakin.edu.au; mwarren@deakin.edu.au

2: Information Risk Analyst
ABN AMRO
ashley.jones@uk.abnamro.com

Abstract

In an environment where commercial software is continually patched to correct security flaws, penetration testing – a form of ethical hacking – can provide organisations with a realistic assessment of their security posture. Penetration testing uses the same principles as hackers do to gain illegitimate access to legitimate authority and thereby verify the presence of software vulnerabilities. Network administrators use the results of a penetration test to correct any flaws and improve overall security. The use of hacking techniques raises several ethical questions that centre on the integrity of the tester to maintain professional distance and uphold the profession. This article discusses the ethics of penetration testing and contributes by categorising them into taxonomy.

Keywords

Penetration testing, computer security and computer ethics.

INTRODUCTION

The adage 'knowledge is power' can be used to illustrate the gap between information security professionals and ordinary end-users. To laymen, information and especially computer security is a clandestine unknown against which they feel powerless. Bereft of security knowledge, end-users succumb to fear, uncertainty and doubt (FUD). The unbridled pace of today's business has underpinned an explosive growth in the adoption of information and communications technologies (ICTs). In an increasingly uncertain and competitive business environment, product life-cycles are shortened and their outputs pushed to market quicker in an effort to maximise profits margins: there are few industries immune to this cycle. Software companies, for example, are pressured to release applications faster and this often results in haphazard software testing practices. In fact, the underlying philosophy of the rapid application development (RAD) 'phased development' methodology centres on finishing core functionality quickly and then implementing other functionality (including security) and rigorous testing in subsequent software versions. The literature shows little convergence enumerating the volume of vulnerabilities routinely discovered every week but commercially the trend remains to be playing a game of 'catch-up' in patching vulnerable software.

In a predominantly networked society these defective ICTs are transmitting vast quantities of sensitive data across relatively unsecured communications media. To compound matters maturing technologies such as encryption can be used to make sensitive data useless to interceptors but it is essentially a patch in itself: the Internet was designed to survive a nuclear assault and not for the widespread commercial use it has adapted to today nor with security in mind. With that in mind, the question facing many network administrators is 'how secure is my network?' Assessing the security of a network can be achieved using controlled hacking techniques. Penetration Testing, as it is termed, can provide security assurances to network administrators. The practice tends toward the patching trend noted but by its very nature – hacking – raises several ethical concerns. This article seeks to raise such ethical concerns and arrange them

into taxonomy. We start by discussing the limited body of literature before presenting a categorised set of penetration testing ethics. The paper is then concluded with directions for future research.

LITERATURE REVIEW

'Quality assurance and testing organizations are tasked with the broad objective of assuring that a software application fulfils its functional business requirements.' (Arkin et al., 2005) The major theme in the penetration testing literature tends toward describing how the tester should conduct their tests according to a plethora of differing methodologies and philosophies using a growing collection of labyrinthine automated tools. The commonly accepted definition of penetration testing is the '…[sanctioned] illegitimate acquisition of legitimate authority.' (Geer and Harthorne, 2002, p.1; Logan and Clarkson, 2005; Thompson, 2005) Geer and Harthorne (2002) point out that penetration testing should be considered an *art* rather than a *science*. The distinction is based on the commonly accepted limitation that penetration testing cannot prove the absence of network vulnerabilities, only the presence of them: therefore a penetration test that fails to uncover any vulnerability is not necessarily a good penetration test result (Arkin et al., 2005). Whereas science relies on the disproving of null hypotheses, penetration testing can at most be a science of insecurity as opposed to a science of security (Geer and Harthorne, 2002).

In this same vein Geer and Harthorne (2002) suggest that if a penetration test fails to uncover network vulnerabilities then it is more likely to create value for the client. The possibility for clients to misunderstand the so-called 'science of insecurity' is thus illustrated and an important question of ethics is uncovered by the bye: the chance of misrepresenting penetration testing and its potential to guarantee security. Geer and Harthorne (2002) go on (p.3) with a cynical view of penetration testing, predicting that it will evolve into more of a quality assurance regime using checklists rather than the art of discovering known and unknown vulnerabilities and providing realistic assessment of software security posture.

To the contrary, there seems to be a movement in the literature toward separating security testing from software quality assurance. In the context of bug reports and quality assurance, however, Arkin et al. (2005) suggest that

> … people often use penetration testing as an excuse to declare victory. When a penetration test concentrates on finding and removing a small handful of bugs (and does so successfully), everyone looks good: the testers look smart for finding the problem, the builders look benevolent for acquiescing to the test, and the executives can check off the security box and get on with making money. Unfortunately, penetration testing done without any basis in security risk analysis leads to this situation with alarming frequency. By analogy, imagine declaring victory by finding and removing only the first one or two bugs encountered during system testing!
>
> (Arkin et al., 2005, p85)

Haphazard penetration testing is giving way to engineering approaches emerging from the literature and will wane when best-practice standards mature and the distinction between security professionals and hackers becomes even more prominent. For example Thompson (2005) describes a novel approach to operational penetration testing where a *threat model* resembling a tree-like flowchart is developed. Network vulnerabilities are then tested according to reusable and evolving threat models. Further, Beznosov and Kruchten (2005) describe modern tactics for assuring software quality:

> A fundamental practice in the assurance business is to keep developers and security evaluators "at arm's length" from each other so that they do not affect each other's ideas. Since security assurance must be completely neutral and objective, its practitioners and the developers should not become too closely involved except during their information gathering sessions. This leads to developers often focusing on the functional development with a "tunnel vision" that becomes quite blind to security flaws.
>
> (Beznosov and Kruchten, 2005, pp. 49-50)

Recently, universities have ventured toward offering security testing courses. While still in its infancy this branch of information management is evolving into a specialised profession that will soon require undergraduate qualification like mainstream computer science. In early pedagogical case studies Tikekar (2003) and Logan and Clarkson (2005) point out that until recently, students were not required to study

computer ethics to graduate. Security professionals who are not educated in computer ethics poses perhaps the fundamental question as Logan and Clarkson (2005) ask 'What happens when universities, such as Marshall University, West Virginia house the state's digital evidence lab for the state police, as well as student computer forensic training labs?' (p.159) Without computer ethics curricula, graduates might be more inclined to abuse and misuse their skills. This scenario could extend to the possibility of al-Qaeda (and similar) recruits enrolling in such courses with the predisposed intention to later launch co-ordinated terrorist attacks on critical information infrastructure.

Penetration testing is an evolving practice and the small but growing body of literature shows that there are many arising issues that need to be addressed before it can mature fully. The literature is rich with methodologies and frameworks, but lacks longitudinal studies that prove their merits. For example, the literature lacks case studies that demonstrate how penetration testing fits into business and military continuity planning. Furthermore, although equivalent international standards such as ISO 17799-2000 are in place a formal Australian Standard for penetration testing as yet does not exist. The following section demonstrates the ethical concerns that arise from penetration testing and shows how they converge on six major themes.

THE ETHICS OF PENETRATION TESTING

The Open Source Security Testing Methodology Manual (OSSTMM) (Herzog, 2003) outlines the 'rules of engagement' which are essentially a set of rules designed to restrict unethical penetration testing practices. While the OSSTMM does not discuss the ethics of penetration testing explicitly, its scope is limited to outlining a methodology for penetration testing. We discuss the ethics of penetration testing in this section using the rules of engagement and those identified in the literature review as reference points.

The six major themes of penetration testing ethics centre on *integrity*, which branches out to *serving and protecting the client* and *preserving the security profession*. These objectives are met by avoiding *conflicts of interest*, the provision of *false positives and false negatives*, and finally *legally binding testers to their ethical obligations in the contract*. We discuss the ethical considerations in each category below.

Serve and Protect the Client and Uphold the Security Profession

Testing should not be performed without the expressed written permission of the client. Whereas in the hacking community attacks occur non-consensually, contractual arrangements must be in place to provide a degree of separation between hackers and security professionals.

There is general consensus in the literature that testers should not rely solely on automated tools but also on their skills. Notwithstanding the tester should be well-versed in computer security and know how their tool arsenal works. Tools should be tested themselves in an isolated laboratory prior to being used in production.

The use of past client's data, with or without permission, should not be used to promote the services of the tester. While it may provide a false positive to the potential client, it could also damage the reputation of the implicated organisation.

The tester should notify the client at the first instance of discovering highly vulnerable flaws as in the case of those that endanger human life. The notification should contain appropriate countermeasures to correct the flaw and minimise dangers to human life and the organisation in general.

The principle objective of penetration testing is to test security measures in a network: there is little point to testing systems known to be highly vulnerable. Testing should not commence until appropriate security has been applied to the system.

The results of social engineering tests should be delivered in summarised and statistical format so as not to implicate individuals. The emphasis is on protecting the client and insulating unknowing employees that might be subject to subsequent embarrassment or termination of employment as a result of the test.

The delivery of the report should be preceded by a notice of delivery. The client, upon receiving the report, should acknowledge that they are in receipt of the report. The curtesy underscores the importance of client

confidentiality. The report will contain an appropriate level of detail of the tests performed, the results and the steps the client should take to improve overall network security.

False Positives and False Negatives and Conflicts of Interest

Penetration tests that fail to uncover vulnerabilities should not be passed up as free services (Geer and Harthorne, 2002; Herzog, 2003). This represents false positives by misrepresenting the penetration testing practice as an assurance of the absence of vulnerabilities.

The tester is ethically bound to serve the customer. This holds true even if it is in the best interest of the customer to engage a different testing company. In that event, the tester should not recommend any particular company so as to avoid the possibility of a conflict of interest or the perception of one.

The promoting of public hacking or trespass contests for security assurance is unethical because it implies a false security guarantee. Contests also draw unnecessary attention to the client network as a perception of a 'fair game' target will endure in the hacking community far longer than the expiration of the testing contract. When new vulnerabilities ensue the client's network may be the target of continuing non-solicited attacks.

As alluded to in the previous sub-section, clients should behave in a manner that does not encroach on the tester or interfere with a test in a manner that may alter its outcome. This includes deploying additional security during a test. As testing provides a snapshot in time of the security posture of a network, changing the security environment could lead to false positives or false negatives. Further, the client should notify only key internal personnel of the penetration test. The extent to which people are kept inside the circle is at the discretion of the client but it must be stressed that widespread knowledge of the test will alter behaviour and affect the outcome of the test thus promoting false positives or false negatives.

If white-box or in-house testing is requested, the tester should first perform black-box testing offsite. This concern draws attention to the use of internal security auditors that could develop tunnel vision (as insiders know the target network very well) and lead to false positives and false negatives. Statistically (AusCERT, 2005; CSI/FBI, 2005), however, system compromise originates in greater frequencies from within the organisation than outside the organisation. In this light the use of internal security auditors presents some merit.

Legally Binding Ethic and Other Considerations

The tester should work non-disclosure and limited liability clauses into the contract. The use of these clauses in the contract legally binds the tester to his ethical obligations. Non-disclosure is common practice, but the tester should also assume limited liability generally not exceeding the cost of the test for inadvertent damages incurred by the client as a result of negligent testing or malpractice. Therefore, it is in the best interests of the tester to have sharpened their skill base to provide the said degree of separation between hackers, script kiddies and security professionals.

Ethically, the contract should scope the tests and indicate emergency contacts as well as the IP addresses from which the tests are originating. Additionally, the contract should specify failsafe procedures such as recovering from DoS attacks.

It has been suggested that using FUD to sell penetration testing services is unethical. The OSSTMM explicates that crime facts and figures should not be used to promote security testing. Academics, however, routinely use crime statistics – such as those found in the recent AusCERT (2005) and CSI/FBI (2005) computer security surveys – to justify the problems with computer security, necessitate new research, and sell security courses at the university and practitioner levels. The question of using statistics as an ethical concern should be met with a balanced view of the need to educate end-users in security versus the instilment of FUD.

The ethical concerns presented in the paper centre on five interrelating themes: serving and protecting the client; upholding the security profession; conflicts of interest; false positives and false negatives; and, legally binding the tester to their professional ethics. A common factor, integrity, can be seen to tie these categories together as in the following figure. The tester's integrity should compel them to serve and protect the client while behaving ethically to preserve the integrity of the profession. The following figure

illustrates our categorisation of penetration testing ethics and how they correlate with a central theme of the integrity of penetration testers.

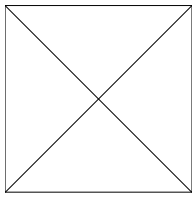


Figure 1: Taxonomy of Penetration Testing Ethics

CONCLUSION:

We have seen that the business world is experiencing unparalleled growth due to its unbridled speed. No organisation is immune to the rapid changes in technological development that can be seen to fuel a cycle of business needs driving technological development enabling business needs. The pressures facing the business environment are felt by software companies too that cull application security testing to release the product quicker and patch later. The problem lies in that vulnerable software is introduced to a hostile commercial environment. Penetration testing provides organisations with a means of assessing their security stance at a given moment in time. Testers and clients must behave ethically: clients so as not to alter test outcomes and testers so as to separate them from the hacking community. The ethics of penetration testing centre on integrity; serve and protect the client and uphold the security profession by behaving ethically.

The small body of literature tends toward presenting methodologies and frameworks for conducting penetration tests, but seldom integrates penetration testing into an overall business model. There seems to be confusion as to how organisations can best gauge value from the services of a penetration test. Risk analysis is a sister topic that is gaining incredible momentum in the literature and should also be integrated with penetration testing to produce an overall model of organisational security testing.

Looking to the future, the authors will investigate and propose methods of integrating penetration testing with the better established risk analysis discipline. We will also look at ways of providing pseudo-dynamic security assurance using automated approaches.

REFERENCES:

Arkin, B., Stender, S. and McGraw, G. (2005) 'Software Penetration Testing', *IEEE Security and Privacy*, January/February 2005, pp.84-7.

Australian Computer Emergency Response Team (AusCERT) (2005) '2005 Australian Computer Crime and Security Survey' vol. 1, AusCERT, Brisbane, Australia.

Beznosov, K. and Kruchten, P. (2005) 'Towards Agile Security Assurance', *Proceedings of the 2004 Workshop on New Security Paradigms*, Nova Scotia, Canada.

Computer Security Institute / Federal Bureau of Investigation (CSI/FBI) (2005) 'Tenth Annual 2005 Computer Crime and Security Survey', vol. 1, CSI, San Francisco, USA.

Geer, D. and Harthorne, J. (2002) 'Penetration Testing: A Duet', *Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02)*.

Herzog, P. (2003) 'Open Source Security Testing Methodology Manual', ISECOM, USA.

International Standards Organization (2005) 'ISO/IEC 17799:2005 – Information Technology – Security Techniques – Code of Practice for Information Security Management', ISO, Switzerland.

Logan, P.Y. and Clarkson, A. (2005) 'Teaching Students to Hack: Curriculum Issues in Information Security', *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education*, St. Louis, Missouri, USA.

Thompson, H.H. (2005) 'Application Penetration Testing' *IEEE Security and Privacy*, January/February 2005, pp.66-9.

COPYRIGHT

Professionalism in ICT: meeting the challenge of ethical dilemmas in the workplace.

Anne Sharma, School of Information Technology, Deakin University, Australia.
asharma@deakin.edu.au
Oliver K. Burmeister, Faculty of Information and Communication Technologies,
Swinburne University of Technology, Australia. oburmeister@swin.edu.au

Abstract
Swinburne University of Technology offers a final year subject that explores ethical issues related to the ICT profession. A major objective of this subject is to consider ethical issues in the workplace. This study reports how the ICT ethics subject has impacted on graduates' capacity to adapt to ethical dilemmas faced in the workplace. The qualitative perceptions of past graduates were obtained via interviews. The interviews focused on ethical issues faced in the place of employment and how useful the Swinburne subject was in dealing with these matters. The strengths and weaknesses of the subject were explored during the interview, providing the basis for future enhancements of the curriculum. A particular focus within the subject is on the Doing Ethics Technique. Further research is needed to better adapt the technique to the needs of professionals in the workplace.

Keywords
Professionalism, Doing Ethics Technique, teaching ICT ethics.

INTRODUCTION
In professional practice today there are many situations where it would be helpful to have a particular way of sifting through issues to determine appropriate courses of action. For example, Preece (2002) said that 'The womb is like an ethical war-zone. Embryonic stem-cell research, deaf lesbians choosing deaf-babies, IVF embryos chosen and conceived to save existing children, single and lesbian women accessing IVF. Hardly a day goes by without a new ethical dilemma. The pace of technological change and precedent makes it almost impossible to keep up.'

Can professionals be taught ethical decision making? Can a student learn to act ethically through tertiary studies? Students entering such courses are often sceptical. To paraphrase them, students say things such as:

- I have learnt ethical behaviour in the home of my parents. One semester here is not going to change years of growing up.
- In the workplace I will be a learner, I will be expected to behave as they do and learn from them. I have no place telling them how to conduct themselves, just because I completed a semester of ICT ethics.

This paper presents the results of a preliminary investigation into the impact of an educational subject taught at a university on professional ethical behaviour. It also explains particular teaching methods used in that subject that have been shown to aid people in ethical decision making (Simpson and Burmeister, 1998; Simpson, Nevile and Burmeister, 2003). Data was collected in interviews to compare the learning outcomes with past graduates, now employed in the Information and Communications Technology (ICT) industry. The paper concludes with suggestions of how the subject and teaching methods can be extended to suit professionals, and to better prepare students for professional life in ICT.

BACKGROUND
At Swinburne University of Technology, 'Professional Issues in Information Technology' (PIIT) is taught to all final year ICT students. It can be taken by students from various Faculties as an elective, although students without industrial experience are strongly discouraged from taking the subject. PIIT is usually the

only subject that incorporates ethics in their computing courses. Despite their lack of familiarity with workplace ethical issues, almost all students, after finishing the subject, rate it as one of the most valuable to their professional development and one of the most enjoyable in their course.

Over the past 15 years the subject has evolved (Simpson and Burmeister, 1998; Simpson, Nevile and Burmeister, 2003). The focus has shifted from straight lectures to exploring real cases that confront professionals in the workplace. Many of these are introduced by guest industry speakers, brought in to demonstrate to students that PIIT topics are ones really faced in professional practice. However, students have often expressed difficulty in thinking through ethical situations. Early attempts to help students in this regard followed a case study approach. Typically with the case study approach, there is an appeal to some standard, such as a code of ethics, a code of professional conduct or a code of professional practice. This approach is common in the literature, for helping professional make ethical decisions (Anderson et. al., 1993; Burmeister, 2000; Bowern, 2003). While this approach is helpful, it is insufficient.

As a result of this the 'Doing Ethics Technique' was developed (Simpson, Nevile, and Burmeister, 2003). This technique builds on the case study approach, by utilising scenario analysis. Although the technique was developed for student use, it is also applicable to industry [as illustrated in an adaptation of the technique reported in Nevile and Burmeister (2003), and Nevile et. al. (2003)]. This paper will discuss an evaluation of graduates of the PIIT subject and in particular the 'Doing Ethics Technique'. It is to be noted that at the time the graduates who were interviewed, left Swinburne University of Technology, the technique had not been defined in terms of the name that is now applied to it, the 'Doing Ethics Technique'. The following section will describe the 'Doing Ethics Technique'.

THE DOING ETHICS TECHNIQUE

The technique of analysis depends upon asking questions. It has been found that the order in which the questions are asked is also important.

Q1 What is going on? – What are the facts?
Q2 What are the issues?
Q3 Who is affected?
Q4 Hence, What are the ethical issues and implications?
Q5 What can be done about it? - What options are there? and
Q6 Which option is best? – and Why?

An injunction to 'think ethically' about a situation is not helpful. Perhaps if one has a background in moral philosophy this would work, but usually both students and ICT professionals require some form of guidance as to how to achieve an appropriate outcome. The technique has proven itself as a means to achieving this.

This approach is not dependent on a particular standard, such as the code of ethics of a particular professional society. It is a technique that can be applied in a variety of circumstances, not limited by technological, cultural or religious background.

The approach is not limited by one's moral philosophy. One can use this technique effectively and be an objectivist, holding that certain moral truths remain good independently of personal likes and dislikes, or a relativist, holding that truths are relative to the individual or one's culture. Similarly, this approach can be used by consequentialists, holding that consequences determine if something is ethical, and by deontologists, holding that some things, regardless of the consequences, are right or wrong in themselves. The technique is a means of arriving at an ethical outcome.

THE SELECTION OF GRADUATES

For this preliminary study into the effectiveness of the ethical teaching for professional practice, a small ethnographic investigation was conducted. For pragmatic reasons a sample of convenience was employed. Many graduates had moved interstate or overseas. Therefore, those known and available were contacted. This convenience sampling is a limitation of the study. A total of five graduates were contacted, including

four males and one female. The 20% female representation is close to the enrolment profile in Bachelor of Information Systems/Bachelor of Information Technology programs at the case study University.

Interview Questions Asked Of Graduates

1. What were the main strengths of the Professional Ethics subject from the perspective of gaining theoretical knowledge regarding professional ethics?
2. What were the main weaknesses of the Professional Ethics subject from the perspective of gaining theoretical knowledge regarding professional ethics?
3. What are the opportunities for improving the subject?
4. Have you ever faced any ethical professional dilemmas at your workplace following graduation?
   If so, please provide some examples of them.
   In the Professional Ethics subject a particular technique, now called the 'Doing Ethics Technique', was employed to help students think through difficult ethical situations. Did you employ the technique and if so what were the results? If you didn't use the technique, what techniques (if any) did you use to resolve ethical situations you confronted?
5. Did the Professional Ethics subject provide you with the necessary knowledge and skills to deal with workplace ethical issues?
   If so, in what way did the subject assist you in dealing with the ethical issue?

The following section will discuss the results of this study.

CASE STUDIES

Graduates interviewed were between 23 and 26 years old and had either completed Bachelor of Information Technology (BIT) or Bachelor of Information Systems (BIS) at Swinburne University of Technology. Four out of the five participants have approximately 3 years ICT work experience including 1 year of Industry Based Learning which was incorporated into their BIT program. The remaining respondent has approximately 2 years work experience.

The reader ought to also be aware of the potential biases of the researchers. One author is a graduate of the BIT program, currently working in the ICT industry. The other author is an academic who has been involved in teaching PIIT from time to time.

Strengths Of The Professional Ethics Subject

Primary strengths of the Professional Ethics subject from the perspective of gaining theoretical knowledge regarding professional ethics were identified as follows:

- Open forum tutes were better than the standard textbook approach as there was enhanced learning through interaction rather than boring textbooks. Additionally, the use of real life scenarios gave the respondent an insight as to how graduates can attack certain workplace situations in the future;
- Debates and presentations were beneficial in terms of building better public speaking skills;
- The subject was comprehensive - the course content extended through a range of ethical issues and topics. Additionally, it highlighted real world issues from an ICT professionals point of view and provided a theoretical framework for a professional to build and develop upon; and
- It was an independent forum to raise ethical issues with the safety and openness that one mightn't get in a work situation.

Weaknesses of the Professional Ethics subject

Core weaknesses of the Professional Ethics subject from the perspective of gaining theoretical knowledge regarding professional ethics were identified as follows:

- There is a lack of industry connection – scenarios are not in the context of work experience and it is less easy to see how the different players might come into it and to consider the pressures of a work situation. Scenarios and role playing roles are ok; however, decisions are somewhat disconnected from the work environment.

- There was a lack of enforcing open participation. There was always a small number of students that interacted in tutes and the others would refrain;
- There is a lack of ability to follow up over the long term and there is no chance to revisit specific issues that have be raised earlier in the course;
- It was unclear in many cases what was a project management issue (poor planning leading to failure) or an ICT issue (poor implementation leading to failure); and
- The subject was mostly theoretical - it gave you a theoretical understanding however dealing with ethical situations in a practical context is different. It is not quite as clean cut and there is more emotional involvement in a workplace situation as well. The subject does not prepare you for that aspect of a workplace situation.

Further improvements to the Professional Ethics Subject
Further improvements to the subject were suggested:
- There should be a heavier weighting on class participation i.e. there needs to be more emphasis on discussions than written content;
- A second year ethics subject should be introduced to the BIT course. A year's gap between the two subjects would be ideal, so that students can review issues identified in the first subject. Hence, students are formulising an ethical conclusion from what they studied earlier rather than what they have learnt themselves;
- The subject should address more general workplace ethical issues instead of just ICT ethical issues;
- The theory did not thoroughly manage what was ethical behaviour, and what was a mistake or an effect of something that could not be foreseen; and
- Introduce a practical task where a student figures out what ethical issue in ICT they are passionate about and present that case in classroom scenario where they are open to being questioned about it, have a debate about it, etc. It is not going to have still the same impact as it will in a real life situation. However, it is probably as close as a student will get to a real life situation in a Professional Ethics subject.

How graduates have dealt with ethical issues and whether they have utilised the 'Doing Ethics Technique'
One participant employed the 'Doing Ethics Technique' when the respondent faced an ethical professional dilemma at the graduate's workplace following graduation. Though the technique was adopted, it was not followed rigorously and in no specific order as detailed below:

Q1 What is going on? – What are the facts?

- The graduate was employed at a company (company1) that was facing receivership;
- An international company (company2) based in Malaysia was born out of company1;
- Shortly before company1 declared itself bankrupt, company2 paid a substantial amount of company1's bills etc., which bought them equity into company1;
- Both hard and soft assets were shipped to Malaysia, including the intellectual property (IP) developed by the graduate; and
- Company2 offered the alumnus a job with them, reengineering Company1's IP to suit their back end software.

Q2 What are the issues?

They were evasive and clear:
- Should the graduate accept a job with a company which obviously was involved in dodgy dealings with Company1?
- Should the graduate then proceed to reengineer Company1's IP to suit Company2's back end software?

Q3 Who is affected?

- Creditors of Company1 who would not receive money owed to them as a result of Company2 'buying' Company1's hard and soft assets;
- Company1's staff that was unaware of the dubious transactions between Company1 and Company2, or even the financial situation of Company1; and
- Company2's staff and the staff that moved from Company1 to Company2, that were unaware of the dubious transactions between Company1 and Company2 and whether Company2's actions were sinister towards Company1.

Q4 Hence, What are the ethical issues and implications?

- Should the graduate continue working for Company1 given the value he represented to Company1?
- Should the participant accept the job offered with Company2 given their risky dealings with Company1?
- Should the alumnus incorporate the source code from Company1 to Company2's back end software?

Q5 What can be done about it? - What options are there?

- The participant can either leave Company1 and work for Company2 or find employment with another company;
- If the graduate accepted the job offered with Company2 the respondent would have the following options:
    - Move to Malaysia and work at the head office; or
    - Stay in Melbourne and work from home.
- The graduate can either choose to incorporate the source code from Company1 to Company2's back end software or not.
    - If not, the respondent can develop a new solution to suit the needs of Company2;

Q6 Which option is best? – and Why?

- Given that no other employment was available, the graduate accepted the job with Company2;
- The alumnus chose to live in Melbourne and work from home, as the respondent felt it was easier to focus
- Incorporating Company1's source code for Company2 would have been unethical; and
- The participant chose to target Company2's requirements and formulate complete documentation without giving away any IP as this seemed most appropriate activity in a business sense. Additionally by following the System Development Life Cycle it would have made the new solution more personalised and better documented for future development.

Other graduates have not followed the 'Doing Ethics Technique' as outlined in the subject. An ethical dilemma that a respondent has faced was a disclosure issue. A manager approached the alumnus and wanted a detailed report of what mobile calls were made, number tracing for the employees landline, whether corporate numbers were being called, and email addresses the employee was communicating with. The graduate did not follow the 'Doing Ethics Technique' in this situation. However, the respondent reviewed the company's ICT policy and subsequent legislation and verified the following:

- Who had the right to the information requested;
- What authorisation was required to access the information requested; and
- Even with sufficient authorisation, whether that information was protected by company privacy policy.

As a result of the participant's investigation, they met with the manger that requested the report and informed them they could not access the information as it would breach company privacy policy.

How The Professional Ethics Subject Has Provided Alumni With The Necessary Knowledge And Skills To Deal With Workplace Ethical Issues

The Professional Ethics subject developed one respondents existing knowledge and skills on workplace ethical issues. The graduate believes that everyone already has essential knowledge and skills to deal with ethical issues. The Professional Ethics subject aided the alumnus in building on framework and background knowledge, and to be confident about a decision concerning ethical issues and cope well with making them. The Professional Ethics subject opened up the area of ethics more as the participant became aware that there were standards and mechanisms one can follow professionally for workplace ethical issues people face daily.

One participant believed that the professional ethics subject provided the graduate with necessary knowledge to deal with ICT ethical issues, but not knowledge to deal with workplace ethical issues. For example, the subject explored stealing code, ideas, hacking, and other issues, but not general ethical issues that ICT professionals would still face, such as the ethics of calling in sick when you are not, taking workplace supplies, lying to bosses, covering up mistakes, redundancies, and more.

The Professional Ethics subject provided an alumnus with a skeleton of knowledge on workplace ethical issues. The subject provided the participant with what they should consider in workplace ethical issues, and who they should contact. However, the subject did not provide the respondent with necessary skills and knowledge to any degree of detail. The graduate believes that they can learn better through practical application of their knowledge than through theoretical study. However, the participant did appreciate the skeleton structure that the subject provided.

ANALYSIS OF RESULTS

The main themes identified in the strengths of the Professional Ethics subject from the viewpoint of acquiring theoretical knowledge regarding professional ethics was the provision of theoretical underpinning of professional ethics. This was balanced by more practical and applied knowledge created not only as a one way process from lecturer to students, but also through student to student and student to staff interactions in classes through the use of scenarios and classroom debates.

Shared themes established in the weaknesses of the Professional Ethics subject from the position of obtaining theoretical knowledge concerning professional ethics, included a perceived need for greater realism including inputs from industry. Additionally, a better balance between the theory–practice continuum, but perhaps being closer to the right of this spectrum would have assisted the ICT graduates to cope better with the ethical dilemmas faced in the workplace.

Improvements in the subject that were commonly identified included the improvement of assessment–weighting more heavily on practical aspects. Furthermore, there should be a greater emphasis on applied practicum/industry than theoretical knowledge in classes.

The ‘Doing Ethics Technique’ does not appear to be widely adopted by graduates. This technique may need to be adapted and/or revised in view of the opinions experienced by the case study graduates.

Overall, the subject appears to have provided adequate knowledge to deal with ICT ethical issues. However, workplace ethical issues were somewhat lacking according to survey participants.

It should be noted that all respondents have only limited employment experience of up to three years. Further, owing to the downturn of the ICT industry most of the participants are working relatively task oriented junior positions with lesser exposure to more complex ethical dilemmas. Most of the graduates felt that there was too much theoretical content in the Professional Ethics subject and expressed a desire for greater practical applications. However, it is clear that the theoretical foundations established from studying the Professional Ethics subject have assisted them to reflect on the concept of ethics when ethical dilemmas arise, thereby facilitating the problem solving. It will be informative to undertake further survey with these students in say five years time once they have reached the management level. Such a study would permit temporal comparisons of ethical dilemmas in the workplace.

CONCLUSION

The results of the survey confirm what has been argued elsewhere (Nevile and Burmeister, 2003; Nevile et al., 2003), that in its passive state, the Doing Ethics Technique does not sufficiently address the needs of people working through ethical dilemmas. Nevile et al. (2003) explored an active variation to the technique in the domain of online accessibility, that may signal the way forward. The Doing Ethics Technique has been an important step forward in guiding *student* ethical decision making, but the results obtained in this study seem to indicate that further refinements are needed to make it useful to the ICT *professional*. Further research is also required to determine if the active variation of Nevile et al. (2003) is a better solution. Nevile et al. (2003) put forward the notion that different stakeholder viewpoints need to be considered in an active way; active being defined as a team-based resolution to ethical dilemmas. Nevile et al. (2003) did not have empirical data to back their ideas, their research was based on a review of the literature and on practitioner conjecture. The first bullet point in the weaknesses section above appears to confirm this notion; that is, a weakness in the Doing Ethics Technique is that different workplace viewpoints are not taken into account. Further work is needed to find an effective solution to this weakness.

One weakness of teaching ethics, identified by participants in the survey, is the lack of follow-through for graduates. An innovative solution here might be something the Australian Computer Society (ACS) did in March 2002. Each year the ACS hold their national conference and in conjunction with it hold a one day series of events for new graduates (those working 12 months or less in ICT) and students. In 2002 this involved an afternoon session where those present (over 100 young people from all over Australia) analysed 2 case studies, with the help of a panel of industry experts. This approach could be the solution to the weakness of follow-through identified by survey participants. That is, rather than individual universities attempting to conduct follow-through with past graduates, wider acceptance and better understanding of the workplace issues, could be achieved through the professional society taking on this responsibility.

REFERENCES

Anderson, R. Johnson D, Gotterbarn D, and Perrolle, J (1993) *Using the ACM Code of Ethics in Decision Making*, Communications of the ACM, Oct.

Bowern, M.E. (2003) *Report to the ACS Management Committee on the ACS Code of Ethics Project*, Sydney: ACS, Dec.

Burmeister, O. K. (2000) *Applying the ACS Code of Ethics*, Journal of Research and Practice in Information Technology, 32(2), 107-120.

Nevile, L. and Burmeister, O.K. (2003) *Acting Accessibility: Scenario-based consideration of Web content accessibility for development and publishing communities*. Proceedings of The Twelfth International World Wide Web Conference, May, Budapest, Hungary.

Nevile, L., Burmeister, O.K. and McCathieNevile, C. (2003) *High Quality Scenarios for Raising Web Content Accessibility Awareness*. Proceedings of HCI International 2003 Conference, June, Crete, Greece.

Preece, G. (2002) *A war-zone in the womb*, The Melbourne Anglican, May, No 393.

Simpson, C.R., and Burmeister O.K. (1998) *New Professionals, New Measures of Worth, New Ethic of Collaboration*, Proceedings of the Fourth International Conference on Ethical Issues of Information Technology, The Netherlands: Erasmus University, March, pp 651-660.

Simpson, C.R., Nevile, L. and Burmeister, O.K. (2003) *Doing Ethics: a universal technique in an accessibility context*, Australian Journal of Information Systems, 10(2), May, 127-133.

COPYRIGHT

Ethics or ICT Governance: Striking an Ethical Balance

Graeme Pye and Matthew J. Warren

School of Information Systems,
Faculty of Business and Law,
Deakin University,
Geelong, Victoria, Australia, 3217

graeme@deakin.edu.au and mwarren@deakin.edu.au

Abstract

Ethics and Information Communication Technology (ICT) Governance both have their place in today's business organisations, but can their practical applications present an ethical ambiguity for the IT professional employed within the business organisation? The guidelines contained within various codes of ethics recommend principles regarding the ethical behaviour of individual IT professionals, while perhaps in contrast, IT Governance as outlined in the new Australian Standard for Corporate Governance of Information and Communication Technology (ICT) (2005) provides ICT governance advice for business. Herein lies the central difference between these two viewpoints within an organisation and this requires further analysis to develop clarity of understanding relating to the perceptive ethical obligations recommended that relate to both the individual and the organisation itself, to identify where an ethical balance may exist.

Keywords

Ethics, IT governance, ICT and ACS.

1. INTRODUCTION

Depending on your personal perspective ethics can have a number of relevant meanings, in general terms ethics is regarded as the moral rationales that influence a person's behaviour or the carrying out of an activity or alternatively, ethics can also refer to the area of knowledge that deals with moral principles (Pearsall 1998).

However, from an information technology (IT) business domain perspective, Clarke's (1999) view was that the term ethics is intended to refer to the guiding principles of doing what is right or wrong from a moral perspective, in reference to ethical behaviour of both the individual IT professional and the governance of an IT department within a business organisation. Even though both views of ethics have merit, from this paper's perspective a deeper understanding of the philosophical foundations of ethics and morality needs to be initially established to refine the research domain.

At the outset it is also pertinent to mention that the previous research of Burmeister (2000) covers in greater detail the Australian interpretation, understanding and application of the Australian Computer Society's (ACS) Code of Ethics by IT professionals, particularly in relation to practical resolution of ethical issues in the workplace. While, this research lightly touches upon this area to 'set the scene', *[sic]* its main focus however will be to investigate and explore the underlaying ethical philosophies, rather than to revisit this research from the Burmeister (2000) perspective.

As an overview, this research seeks to investigate and philosophically appreciate the ethical perceptions, interpretations, principles and professed tenets of the ACS Code of Ethics (2003), while also investigating the genesis and potential influence of IT governance in light of the recent publication of the Australian Standard for the recommended guiding principles of Corporate Governance of Information and Communication Technology AS 8015-2005 (2005).

As a result of this circumstance, the IT professional is now potentially faced with two behavioural conventions in the workplace that can both exert their own normative influences on the employees' ethical behaviour. So initially this paper will explain and philosophically define ethics and morality, before proceeding to examine and compare the particular focus of the key principles underpinning the ASC Code of Ethics (2005) and the Australian Standard for ICT Governance (2005).

Then from this examination, determine the ethical voicing used in the respective documents before expanding and drawing some initial conclusions on the potential interaction between the ACS Code of Ethics (2003) and the ICT Governance Standard (2005) from the ethical and moral perspective of the IT professional.

2. PHILOSOPHY OF ETHICS AND MORIALTY

According to the Oxford Dictionary of Philosophy, ethics is 'the study of the concepts involved in practical reasoning: good, right, duty, obligation, virtue, freedom, rationality, choice' (Blackburn p.126 1994) while, applied ethics is 'the subject that applies ethics to actual practical problems …' (Blackburn p.126 1994). Furthermore, the ethics and morality of an individual or people can be regarded as the same thing according to Blackburn (1994), however a usage of morality by German philosopher Kant (1724 – 1804) restricts the usage of morality to ideas of duty, obligation and principles of conduct, while reserving ethics for the Aristotle (384 – 322 BC) approach of practical reasoning pertaining to the ideas of virtue and generally avoiding the separation of moral considerations from other practical considerations.

These philosophical rationales will form the basis of a philosophical analysis from an ethical and moral perspective of the information content of the ACS Code of Ethics (2003) and the ICT Governance Standard (2005) respectively, to gain a deeper understanding of their philosophical basis, considered roles and application within the IT domain of any business organisation.

3. CODE OF ETHICS

Many computing codes of ethics abound and are generally based around a number of perceived ethical or moral principles that provide guidance and engender a commitment toward ethical behaviour that is appropriate for and expected of IT professionals. For example, the following list illustrates a several societies or associations that have their own codes of ethics or codes of conduct that are available to both their members and the public:

- Association of Computing Machinery (ACM 1997) ;
- Australian Computer Society (ACS 2003)
- British Computer Society (BCS 2005);
- Computer Ethics Institute (CEI 2001).

Generally, such codes are used as guiding principles for professional computing industry associations' as a resource for their members and as a means of outlining the ethical expectations of both the association's membership and individual IT professionals in general. The ACS's Code of Ethics (2003) is one such code that is obviously applicable to the Australian IT industry environment and will therefore be the focus of this enquiry.

3.1 ACS Code of Ethics

The ACS Code of Ethics (2003) document delivers ethically based behavioural recommendations that are strongly focused on delivering sound ethical and moral advice to individual IT professionals that are members of the ACS, while also providing a reference resource that addresses the following ten principles:

1. Honour and Dignity;
2. Personal Commitment;
3. Values and Ideals;

4. Standards of Conduct;
5. Priorities;
6. Competence;
7. Honesty;
8. Social Implications;
9. Professional Development;
10. IT Professional Behaviour.

The ACS Code of Ethics (2003) seeks to deliver advice that is ethically right in relation to the appropriate ethical behaviour expected of an ACS member or for any IT professional that would be reasonably expected to deliver in their professional work. Although the code addresses a wide area of principles, the advice only serves as guidance to the IT professional from a personal behaviour aspect and does not seek to deliver a methodology for resolving ethical dilemmas between individuals or an individual and the business practice or goal. This is not to say that the individual could not practically reason for themselves what is ethically right or the morally appropriate behaviour to follow with due consideration of the situation, it is just that no specific guidance is given to the reader of how such an ethical issue could be resolved.

From a philosophical standpoint the ACS Code of Ethics (2003) uses an applied ethics approach to addressing the ten principles listed, and what the code is trying to achieve is that in regard to the code's stated principles: these are the suggested ethical behaviours and obligations that can be practically applied by an individual, in order to be regarded or deemed as acting ethically in respect to the ACS Code of Ethics (2003).

It is therefore the view of the authors that from an ethical and moral perspective of the difference between right and wrong that the ACS Codes of Ethics (2003) can guide IT professional to 'do the right thing' *(sic)* and this also suggests that such adherence to the moral and ethical principles as laid out in the code would serve the IT professional well from human-centric, behavioural and interactive perspectives. An additional advantage of this individualistic focus is that it can also be used to promote a bottom-up style of management within a business organisation, where the ethical and moral beliefs of the IT employees within the business organisation may actually, influence or drive the ethical practices of the business and therefore the governance of IT business practices.

4. ICT GOVERNANCE

According to the OECD (2004), the principles of corporate governance should reflect the set of relationships between an organisation's management, board, shareholders and other stakeholders to constitute the rights, roles and equitable treatment of shareholders; disclosure and transparency; and the responsibilities of the board. Additionally, corporate governance should be based on sound strategic guidance of the business, effective monitoring of management by the board and accountability of the board to stakeholders. This involves the responsibility of the board in critiquing and determining corporate strategies, measuring and monitoring the management's performance targets and also securing the integrity of the commercial enterprise system.

Likewise the Australian Standard for Good Governance Principles AS 8000-2003 (2003) reflects the OECD intent and builds further upon other principles covering authority, accountability, stewardship, leadership, direction and how control is exercised within an organisation. In taking governance one step further, the new Australian standard for Corporate Governance of ICT AS 8015-2005 (2005) is a supporting standard that applies to the governance of IT resources and associated technologies used to provide information and communication services within a business organisation. This standard delivers guiding principles within a framework that can empower directors, owners and senior managers in the effective, efficient and control of ICT within the organisation to deliver direction to the management of ICT departments in such a way as to advance good corporate governance principles for the management of ICT assets and persons within business organisations of any size. Therefore the ICT governance standard provides guidance that allows organisational directors and managers to dictate how ICT assets will be

managed to ensure that they support the business goals set by the business owners, management or Board of Directors that are applicable to the principles of good ICT governance.

4.1 Advantages of ICT Governance

As IT technology has become an ingrained and essential part of the enterprise management of transactions, information storage and knowledge management of enterprises, their subsequent dependence on technology has become fundamental to supporting, sustaining and growth of business enterprises. However, the risks associated with ICT become more apparent when considered in the context of doing business on a global scale, twenty-four hours a day, seven days a week, with the reliance placed in ICT resources to provide a competitive edge this can determine the very survivability of the business and ongoing prosperity (ITGI 2003).

Broadbent (2003) views the governance of IT as a high-level managerial activity based on assigning decision rights and developing an answerability framework within the enterprise that focuses on the behaviour and desirable use of IT. Broadbent (2003) further contends that IT governance is about who is qualified to undertake major decisions, who contributes, the accountability of implementing such decisions and the importance of appreciating and understanding the subtle difference between IT governance and IT management. IT governance is about making the strategic decisions, while IT management involves implementing specific IT decisions. Broadbent (2003) further states that good IT governance should comprise of three essential elements: what decisions have to be made; who makes them; and how they are acted upon.

Furthermore, the research of Weill and Ross (2004) has defined ten key principles essential to effective IT governance that are as follows:

1. Actively design governance and continue to provide adequate resources, support and attention;
2. Know when to redesign and adjust the governance systems;
3. Involve senior managers in committees, decisions and performance reviews;
4. Make choices that are business strategic and manageable;
5. Clarify the exception handling process to deal with the unexpected;
6. Provide the right incentives that rewards alignment to the strategic business goals;
7. Assign ownership and accountability for IT Governance to ‘champion’ the process;
8. Design governance at multiple organisational levels;
9. Provide transparency and eduction;
10. Implement common mechanisms across the six key assets:
    - Customer relationships;
    - Product assets;
    - Human assets;
    - IT assets;
    - Physical assets;
    - Financial assets;

These ten principles represent the key outcomes of Weill and Ross’s (2004) research and strongly supports the case for IT Governance as this research also affirms that businesses with effective IT governance programs in place, have attained twenty percent higher profit margins than those businesses with poor quality governance programs that have similar strategic goals.

Therefore in the Australian context, the Australian Standard for Corporate Governance of ICT AS 8015-2005 (2005) is focused on promoting effective, efficient and the acceptable use of ICT by being 'the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation.' (Standards Australia p.6 2005).

4.2 Ethical Focus of ICT Governance Standard

The ICT Governance Standard (2005) document outlines six principles that establish well defined responsibilities for effective ICT governance of Australian businesses (Standards Australia 2005):

1. Establish clearly understood responsibilities for ICT;
2. Plan ICT to best support the organisation;
3. Acquire ICT validly;
4. Ensure the ICT performs well whenever required;
5. Ensure ICT conforms with formal rules;
6. Ensure ICT use respects human factors.

On closer examination the six principles address the management and control of the ICT assets within a business and purport that by following the six principles a business would achieve good corporate governance of ICT. However, they only extend to the actions needed to implement the principles to evaluate; direct; and, monitor ICT governance and do not deliver any sound ethical guidance for individual IT professionals within the business. Although it could be interpreted that principle six alludes to the ethical needs of the people within the ICT process by taking into consideration their concerns and needs, it is unclear how this is managed or achieved from an ethical perspective.

Although the ICT Governance Standard (2005) does deliver a framework for business to follow that suggests how to managerially control IT within the business from a top-down perspective by engendering a view of compliance for good governance of ICT However, the standard does not deliver any framework or methodology to resolve ICT governance issues within the business and therefore such decisions are deferred to the ethics of the employee to resolve within the business context, as principle five directs that "Directors should direct that all actions relating to ICT be ethical" (Australian Standard p.12 2005). Furthermore, as Da Cruz (2004) noted that while varying ideas and perceptions exist about ICT governance, it is still essentially left to the individual enterprises to develop, adapt or address these principles in such a fashion that best meets the business goals.

From a philosophical prospective the ICT Governance Standard (2005) is based in the traditional ethics approach by focusing on the ideas behind what is deemed good governance from the practical reasoning aspect of what is right, dutiful and obligatory across the governing tasks of evaluating, directing, and monitoring as recommended in the Standard.

4.3 ICT Governance and the ACS Code of Ethics

In review, the Australian Standard for the governance of ICT is ethically vague at the personal level and has been developed with a corporate aspect that prescribes what is deemed as necessary corporate behaviour to achieve good governance of ICT. According to the standard, this can be achieved within a business organisation and with top-down management principles that originate at the Board of Directors level and therefore the ICT Governance Standard (2005) applies a high-level view of compliance through the establishment of checks and balances in evaluating, directing and monitoring of the ICT assets within the business, while providing no moral or ethical guidance to the individual IT professional within the business.

We can conclude that governance of ICT as applied can deliver good governance for the management of ICT, but this does not necessarily reflect the ethical standards required by individuals within the business or at the Director level. Therefore we cannot assume that good governance of ICT will necessarily imply the presence of ethically virtuous employees doing what is right within the business.

Furthermore, the ACS Code of Ethics (2003) takes a human-centred focus to providing ethical guidance to IT professionals that is didactic in nature and is achieved by explicitly directing the reader on what is deemed as acceptable ethical behaviour, however it is also pays little regard to the management issues that are the focus of the ICT Governance Standard (2005).

This difference of document focus is also borne out in the use of language and voicing within the respective documents and this relates to corporate and personal voicing used in the respective documents to focus the reader on their particular intent.

5. THE DOCUMENTAL ETHICAL VOICINGS

Melsar and Byrne-Armstrong's (2000) research identified corporate voices and personal voices as being the two distinct discourses that were competing for dominance of the Internet, with each identifying different ethical issues as being the most important to the Internet. Melsar and Byrne-Armstrong go on to establish that the two discourses exhibit differing values and visions of the Internet, such as: the corporate vision as being an extension of property and income generation; while the personal voice is regarded as an extension of creativity and connection between humans.

Likewise we can identify a similar use of corporate and personal voicing being employed in the ACS Code of Ethics (2003) and the ICT Governance Standard (2005) documents. This is evident in the ACS Code of Ethics (2003) where the document voicing using the first person presents the reader with the more humanistic tone of personal voicing that is focused at addressing the individual. While conversely, the ICT Governance Standard (2005) uses an instructive and impersonal tone in the third person that presents the language of corporate voicing, which also presents a formal and measured tone in regard to document content for guiding professional corporate behaviour.

The particular voicing used in these documents is intended to address a particular target audience and therefore the primary focus of the ICT Governance Standard (2005) is that as an officially sanctioned Australian Standard, it is focused on delivering sound practical advice that can assist business in managing in a top-down process, the control and management of IT assets and personal within their respective business organisation. Conversely, the ACS Code of Ethics (2003) delivers ethical suggestions that are directly focused on empowering the individual with ethical advice to enable an IT professional to decide upon the appropriate professional behaviour for their particular ethical situation. The ACS Code of Ethics (2003), from this prospective promotes a bottom-up style of management that encourages the IT professional to drive ethical behaviour for themselves, their colleagues and perhaps ultimately the ethical behaviour of the business organisation.

This difference of documental approach to managing individual ethics from the bottom-up and the ICT governance of business from the top-down, may potentially create an ethical dilemma in itself between the adopted code of ethics of the individual IT professional and the ICT governance requirements of the business. Therefore further investigation is required into the resultant consequences of ethical decisions taken and if contradiction exists, to bring together individual ethical beliefs based on the ACS Code of Ethics (2003) and also the obligations of the ICT Governance Standard (2005), to develop a resolution framework to determine a conciliatory and ethical solution that represents the best intentions of both the individual and the business.

6. CONCLUSION

Upon reflection we have determined that there is a marked philosophically ethical difference between the ACS Code of Ethics (2003) and the ICT Governance Standard (2005) that is due in part to the localised focus taken by each of the respective documents. There exists with little or no regard given to the potential influence of each, their effect upon the business or individual in regard to their application, the potential risks for creating conflictive ethical dilemmas or any in-depth consideration given to determining ethically balanced decisions in regard to both their respective applications.

While, the ACS Code of Ethics (2003) takes a very humanistic and personal view in delivering ethical advice that is based upon the philosophy of applied ethics by employing ethical solutions practically. Conversely it was determined that the ICT Governance Standard (2005) takes an impersonal view that is

focused on the recommended business management aspects of evaluating, directing, and monitoring business processes with a more traditional ethical view of complying to what may be deemed as good governance.

Therefore due to the nature of the philosophically ethical difference between the code of ethics and ICT governance and the real potential for ethical dilemmas to arise, further research is needed to recognise, address and determine such ethical resolutions by better understanding the consequential effects of such decisions made. To do this from an ethical and moral perspective we need to understand the moral theory behind the consequences of ethical decisions and solutions, before developing a framework to guide ethical resolution of issues between the ACS Code of Ethics (2003) and the ICT Governance Standard (2005).

Once this ethical framework is established, the next step in this research is to test the framework against real-world or hypothetical case studies to determine the effectiveness of the framework in addressing and resolving ethical issues between individuals and businesses through the application of applying the philosophical principles of consequentialism.

7. REFERENCES

ACM 1997, *ACM Code of Ethics and Professional Conduct*, (Online), Association of Computing Machinery, Inc., Available from: <http://www.acm.org/constitution/code.htm> (June 2005).

ACS 2003, *Australian Computer Society Code of Ethics*, (Online), Australian Computer Society, Available from: <http://www.acs.org.au/about_acs/acs131.htm> (May 2005).

BCS 2005, *BCS Code of Conduct*, (Online), British Computer Society, Available from: <http://www.bcs.org/BCS/AboutBCS/codes/conduct/> (May 2005).

Blackburn S. 1994, *The Oxford Dictionary of Philosophy*, Oxford University Press, Oxford U.K.

Broadbent M. 2003, The Right Combination, (Online), CIO Online Magazine, Available from: <http://www.cio.com.au> (August 2004).

Burmeister O. K. 2000, 'Applying the ACS Code of Ethics', *Journal of Research and Practice in Information Technology*, vol.**32**, no.2, pp. 107-120.

CEI 2001, *The Ten Commandments of Computer Ethics*, (Online), Computer Professionals for Social Responsibility, Available from: <http://www.cpsr.org/issues/ethics/cei> (July 2005).

Clarke R. 1999, *Ethics and the Internet: Cyberspace Behaviour of People, Communities and Organisations.*, (Online), ANU, Available from: <http://www.anu.edu.au/people/Roger.Clarke/II/IEthics99.html> (June 2005).

Da Cruz M. 2004, 'Australian Standard for corporate governance of ICT', *Information Age*, April/May, pp.10.

ITGI 2003, *Board Briefing on IT Governance*, 2nd Ed., IT Governance Institute.

Melser P. Byrne-Armstrong H. 2000, 'Corporate Voices, Personal Voices: The Ethics of the Internet.' in *2nd Australian Institute of Computer Ethics Conference (AICE2000)*, Australian Computer Society, Canberra, ACT.

OECD 2004, OECD Principles of Corporate Governance, OECD, Paris, France.

Pearsall J. (Ed) 1998, The New Oxford Dictionary of English, Clarendon Press, Oxford.

Standards Australia 2003, *Good Governance Principles. AS 8000-2003*, Standards Australia, Sydney, NSW.

Standards Australia 2005, Corporate Governance of Information & Communication Technology. AS 8015-2005, Standards Australia, Sydney, NSW.

Weill R., Ross J. W. 2004, IT Governance, Harvard Business School Press, Boston, Massachusetts.

COPYRIGHT

RFID and Ethics

Caroline Chan and Matthew Warren

School of Information Systems,
Deakin University, Australia.

Email Contact: carchan@deakin.edu.au

Abstract

Although Radio frequency identification (RFID) has been used for many years in the non-retail areas, the issues associated with its use have never been raised as major concerns until recently. The introduction of RFID into the retail markets, which bring the technology closer to the end user consumers, has then sparked various privacy and legal – related debates. Most of these discussions, however, relate to the legality of collecting and keeping consumer's, possibly, private information and little studies has questioned the social and ethical aspect of the applications of the technology. This paper analyse the nature and social impact of RFID technology and argue that policies or guidelines may be needed to justify the ethical use of the technology.

Introduction

RFID has unlimited potential benefits but at the same time has brought so many privacy-related issues. RFID has been hailed as one of the most revolutionary technologies and has been described as "quantum lead" over the more traditional automatic data capture technology; barcode (Kelly and Erickson 2005).

The applications of RFID technology in the non-retail industry such as military, transport and animal registration is not new. In Australia, some examples of RFID applications are (i) City Link in Melbourne and e-Toll in Sydney (ii) Cats and dogs registration and (iii) E-Passport (to be introduced on 23 October 2005). There are currently very limited applications in the retail items. Several organisations in the US such as Benetton, Calvin Klein and Gillette have initiated the use of RFID for their retail items (Hum 2001; Jones, Hill et al. 2004; Jones, Hill et al. 2005). Wall Mart, the largest retails chain in the US, has requested their suppliers to apply RFID tags on their supplied items (Smith 2005). Cases and pallets from eight suppliers now are being shipped to Wall Mart distribution centres and local stores with RFID tags attached. The company is anticipated to spend around 3 billion dollars for the RFID implementation (Gilbert 2003; Sullivan 2004).

With the fierce uptake of the technology, it is perhaps now the time for the business community to pause and consider the ethical aspect of its implementation as ignorance may cause consumer backlash. The reason for the consumer backlash is the fact that the technology is new, transparent, e.g. consumers may not be aware that RFIDs are being used and the problem of scalability, for example. RFID tags can be very small or large, therefore they can be used in items of clothing, cars e.g. E-tags.

Past papers have mainly discussed the benefits of the technology (see for example (Ollivier 1995; Karkkainen 2003; Sullivan 2004; Jones, Hill et al. 2005; Prater and

Frazier 2005; Wiland 2005) and the legality of collecting consumer information (see, for example (Jones, Hill et al. 2004; Kumar 2004; O'Callaghan 2005) and neglecting the ethical aspect of the implementation. In this paper, therefore, we endeavour to contribute to what we perceive as a gap in the whole discussions of RFID, that is the social implications and ethical consideration of the technology uptake. We describe briefly the technology, its benefits and the potential applications of the technology. The major discussion of the paper concerns the social implications and the ethical aspects of RFID technology.

RFID Technology and the benefits

Radio frequency identification (RFID) was introduced many years ago and provides the ability to track moving objects in various environments where ordinary data capture systems such as bar code labels, could not survive. RFID uses a semiconductor chip, called RFID tags, which can be applied on any item to store data. Data is transmitted from, or written to the tag when it is exposed to radio waves with correct frequency generated from an RFID reader. An RFID tag has an antenna to enable this transmission. The reader converts this data into a form that can then be passed on to computers to process the information.

The RFID tags can be either active (has its own battery) or passive (using power from the RFID reader). *Active tags* are powered by an internal battery and typically have a read or write capability (i.e. the tag data can be rewritten and modified). Some systems operate with up to one megabyte of memory, which allows the tags to store large amounts of data and information such as the tagged part's history. The disadvantages of the active tag are the bigger size, the greater cost, and a limited operational life depending upon operating temperatures and battery type. *Passive tags* operate without a separate external power source. The tags obtain operating power from the reader. Consequently, passive tags are lighter, less expensive, and offer a virtually unlimited operational lifetime. The disadvantage is that passive tags have shorter read ranges than active tags and require a higher powered reader. Read-only tags are typically passive and are programmed with a unique set of data that cannot be modified.

Three major advantages of RFID systems are:

- the non-contact, non–line of sight nature of the technology. Tags can be read through a variety of substances such as snow, fog, ice, paint, crusted grime and other visually and environmentally challenging conditions, where bar codes or other optically read technologies would be useless. With this degree of visibility, it is possible capture the data of an entire pallet or truckload of material in seconds by only passing the products through an RFID reader.
- Read/write capabilities allowing changes to the stored data and its ability to do this speedily (i.e. it can respond in less than 100 milliseconds). This capability is a significant advantage in interactive applications such as work-in-process or maintenance tracking.
- Ability to simultaneously read many tags making it perfect for various applications such as transport, baggage handling, security, etc.

RFID frequency and standards

RFID systems operate on a range of frequencies and require licences for high power implementation. For example, the Australian Communications and Media Authority (ACMA) has just issued an experimental licence for the deployment of high power (i.e. 4 Watt) RFID reader in the frequency range 920-926 MHz to GS1, the RFID standards body in Australia. Generally, however, there are two types of frequency used in the RFID applications —low frequency and high frequency.

- Low-frequency (30 KHz to 500 KHz) systems offer short reading ranges but lower system costs. They are commonly used in security access, asset tracking, and animal identification applications.
- High-frequency (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) systems offer long reading ranges (greater than 90 feet) and high reading speeds, but higher system costs. They are commonly used for applications which require high performance such as railroad car tracking and automated toll collection.

Like with the barcode technology, the application of RFID in a supply chain is also administered by industry standards such as an Electronic Product Code (EPC). All information associated with an EPC can be stored in the EPC Network, which is only accessible to authorized users. The Electronic Product Code (EPC) Network allows unique items or products to be identified, thus enabling companies to achieve true visibility of their supply chain in real time.

RFID Applications

The unique features of RFID have offered unlimited possibilities of industry applications. The two main barriers commonly cited in many RFID papers, costs and the size of the tags, are no longer the case. The price of RFID tags has been dropped to as low as 10 cents a piece (Smith 2005) making RFID tags an affordable technology to be implanted in most items. The size of the tags is no longer an issue. RFID tags can now be mass-produced to the size of a grain of sand, enabling it to be applied to an item of any size. With these barriers overcame, RFID technology is no longer an expensive technology and various industries are racing to undertake the pilot expecting major benefits in the near future.

RFID, security and ethical issues

The following are some ethical problems of where RFID issues could be found.

Security and privacy issues

Security can be a major issue in the implementation of RFID-based technology. Using the passive tags, the power comes from the receiver/reader. This system allows data/information to be easily stolen using a sniffer or power source. You could have the scenario of a thief walking down the streets to check which house has the most valuable goods.

A possible way of overcoming the previous scenario is by using an authentication process in order to access data, or the use of cryptography to ensure that plain text cannot be accessed by unauthorised persons.

Privacy has also become a major concern with the implementation of RFID in the item level. In fact, several technology patents were filed, for example:

- A blocker tag – to disable readers to read tags once the good has been paid (currently only a research project)
- Pseudonym throttling applications – tags would only be readable for every few seconds.

Intelligent chips or spy chips

Intelligent chips – The unique features of RFID have earned a reputation of "intelligent chips".

An extreme view to totally ban the use of RFID tags in any applications has been proposed by a US based organisation, Consumer Against Supermarket Privacy Invasion and Numbering (CASPIAN). They see RFID tags as not only the intrusion of privacy but also believe on the possible health hazard (http://www.spychips.com/). They further called for a boycott to supermarket items implanted with RFID tags (http://www.nocards.org/).

Consumer rights

The legal rights of the consumers in regard to the applications of RFID tags have been discussed by various authors, Simson Garfinkel of MIT (Garfinkel, 2002) proposes "The RFID Bill of Rights" which consists of five "voluntary" rules governing the application of RFID to retail item:

1. The right of the consumer to know what items possess RFID tags
2. The right to have tags removed or deactivated upon purchase of these items
3. The right of the consumer to access of the data associated with an RFID tag
4. The right to access of services without mandatory use of RFID tags
5. The right to know when, where and why the data in RFID tags is accessed.

Other issues

Another ethical concern is that data could be stored overseas (i.e. in the case of off-shore outsourcing) therefore avoiding Australian consumer protection and privacy law.

One way in which many of the ethical issues can be resolved, is by retailers ensuring that tags are inactivated or switched off at the point of sale. This though poses the question, will retailers want to do this?

Conclusion

There is huge potential for RFIDs to be implemented in many Australian organisations, to those selling consumer products to supply chain management situations. There is a major issue about whether the ethical dilemmas will hinder the extent to which RFID will be implemented. There is need for policies and guidelines for the implementation and management of RFIDS and the work by Garfinkel (Garfinkel, 2002) is a starting point but what is needed is an Australian framework to protect and reassure Australian consumers and businesses.

References

Garfinkel, S. (2002). An RFID Bill of Rights,
URL: http://www.technologyreview.com/articles/02/10/garfinkel1002.asp
Accessed: 10th August, 2005.

Gilbert, A. (2003). Wal-Mart to spend $3bn on RFID tracking tags.
URL: http://www.silicon.com/hardware/storage/0,39024649,39116816,00.htm
Accessed: 2nd August, 2005.

Hum, A. P. J. (2001). "Fabric Area Network - A New Wireless Communications Infrastructure to Enable Ubiquitous Networking and Sensing on Intelligent Clothing." Computer Networks **35**: 391-399.

Jones, P., C. C.-. Hill, et al. (2004). "Radio Frequency Identification in Retailing and Privacy and Public Policy Issues." Management Research News **27**(8/9): 46-56.

Jones, P., C. C.-. Hill, et al. (2005). "The Benefits, Challenges and Impacts of Radio Frequency Identification Technology (RFID) for Retailers in the UK." Marketing Intelligence and Planning **23**(4): 395-402.

Karkkainen, M. (2003). "Increasing Efficiency in the Supply Chain for Short Shelf Life Goods using RFID Tagging." International Journal of Retail & Distribution Management **31**(10): 529-536.

Kelly, E. P. and G. S. Erickson (2005). "RFID Tags: Commercial Applications v. Privacy Rights." Industrial Management & Data Systems **105**(6): 703-713.

Kumar, R. (2004). "Interaction of RFID Technology and Public Policy."
URL: http://www.wipro.com/insights/rfidtechnology.htm
Accessed: 2nd August, 2005.

O'Callaghan J (2005) RFID and the Law: Demystifying the Myth, Key Notes: Vision in Progress: Global Standards and RFID Conference, Melbourne, July.

Ollivier, M. (1995). "RFID Enhances Materials Handling." Sensor Review **15**(1): 36-39.

Prater, E. and G. V. Frazier (2005). "Future Impacts of RFID on e-supply chains in grocery retailing." Supply Chain Management - An International Journal **10**(2): 134-142.

Smith, A. D. (2005). "Exploring Radio Frequency Identification Technology and Its Impact on Business Systems." Information Management & Information Security **13**(1): 16-28.

Sullivan, L. (2004). Wal-Mart Outlines RFID Expansion Plans. Information Week.

Wiland, E. (2005). RFID: Revolution in Logistics or BigBrother Technology? CIO.
URL: http://www.cio.com.au/index.php/id;1836480571;fp;4;fpid;21
Accessed: 2nd August, 2005.

COPYRIGHT

Issues of Australian IT Security Outsourcing

Sneza Dojkovski[1], Matthew Warren[1] and William Hutchinson[2]

[1]School of Information Systems,
Deakin University, Australia.

[2]School of Information & Computer Science,
Edith Cowan University, Australia.

Email Contact: sneza.dojkovski@deakin.edu.au

Abstract

IT security outsourcing is the establishment of a contractual relationship with an outside vendor to assume responsibility for one or more security functions. The decision making process associated with outsourcing security is complex. To improve the effectiveness of the decision making process a conceptual model that integrates security benefits, costs and their respective performance measures will be developed. This model will support management in their aim of overseeing IT security effectively. The research will make a valuable contribution towards determining the impact of IT security outsourcing within Australia.

INTRODUCTION

Information systems have become an integral means of doing business over the past few years, making them one of the most valuable assets companies possess, offering availability, security, and good performance. As a result, companies are now forced to find ways to secure that asset. To meet these challenges, organisations are increasingly considering outsourcing of their information systems activities as an attractive option. There are three ways to accomplish the security of an organisation's assets. The company can perform all tasks in house; hire an outside company or companies to perform all security related tasks, which is outsourcing, or some combination of the two [Faile 2001]. The primary focus of this paper is outsourcing security services and therefore most of the discussion will reflect that, though some mention of the other two options will be put forth.

Outsourcing can be simply defined as an arrangement in which one company provides services for another company. These services are ones which typically could be handled in-house, but which are for various reasons turned over to another company or companies. It follows then that security outsourcing can be defined an arrangement in which one company provides security services for another company [Faile 2001].

Increasingly, organisations are looking offshore for the means to minimise IT service costs and related taxes. Security outsourcing is also a common option for start-up organisations and for those entering new lines of business. Instead of devoting time, energy and finances, organisations believe they can minimise the start-up time required to enter new markets by contracting an outsourcing organisation to provide those services immediately [CICA 2003]. Much has been written about Outsourcing as a management tool [Burnett, 1998, James and White 1996, Johnson, 1997] but less has been written about the ethical issues.

This paper presents a perspective on the matters that an organisation addresses when considering IT security outsourcing as an option and the ethical issues. It is intended to address the benefits and challenges of security outsourcing aiding in the development of a conceptual model that will improve decision making for management when they make or examine outsourcing decisions.

WHY OUTSOURCE SECURITY

There are many issues for management to consider when making the decision whether to outsource security or keep it in house. Difficulties associated with hiring and training of skilled professionals, retaining these professionals, cost, continual technological advances, increasing threat from outsiders, legal considerations and peace of mind are all considerations [Faile 2001]. The following paragraphs identify some of the reasons an organisation can decide to outsource their security services [CICA 2003]:

Operational Benefits

Personnel

It is very difficult today to find qualified personnel to fill key positions in the security field. Security is an emerging profession and the supply of qualified personnel is limited. If an organisation is able to find qualified personnel they may not be able to meet their income demands, and many larger companies need more than three of these people [CICA 2003].

Training personnel

When an organisation is able to hire qualified personnel, they will require training as advances in technology are made, which will further increases the cost. After they have received suitable training, they become more marketable and move into organisations which can meet their high income demands [CICA 2003].

Technological Benefits

Technology is rapidly advancing and security techniques and technologies along with it. VPN equipment, Intrusion Detection Systems, firewalls, routers, operating systems, penetration testing tools, and DNS are a few of the technologies that security professionals must be able to learn and have training regarding. All of the technologies involved in security require vast amounts of knowledge and expertise to properly utilise them. This requires finance be allocated to training as well as the purchase of products [CICA 2003].

Cost Benefits

Cost is a very important factor when deciding whether to outsource security. As mentioned previously, the cost of in house expertise can be high. Security technologies can be quite expensive and as technology advances organisations have to continuously upgrade which furthers the cost.

Many organisations, especially Small and Medium Enterprises (SME's), are not able to hire the security professionals they need, given their limited budgets. Instead, they either rely on their IT staff to perform security functions or have an understaffed security office to perform security functions. However, security is a full time responsibility and will suffer if not properly looked after. This improper staffing may lead to security flaws that may open an organisations network up to attack. By outsourcing these services, an organisation can get back to its core business functions [CICA 2003].

CHALLENGES TO SECURITY OUTSOURCING

Security outsourcing is based on gaining the benefit of expert or specialist knowledge and competency. Yet the risk exists that the knowledge and services outsourcing providers offer, may not be matched by the needs of the organisation. Consequently, security outsourcing operations manages some risks and creates new risks to manage [Aalders 2001].

The following paragraphs examine some problems that may arise when outsourcing:

Operational Problems

Control

Organisations fear they will lose control over vital information or processes once its security requirements are managed by an outsourcing provider. One of the problems in justifying the outsourcing of the organisation's security needs and services is the fear of losing control and flexibility of these services. Control of outsourced functions and operations can be maintained by closely scrutinising the provider's reputation, investigating the quality of services provided, incorporating performance measures in agreements, etc [Aalders 2001].

Outsourcing also creates a need for new management skills. As the organisation no longer has direct control over security applications, it must exercise indirect control through effective management, governance and monitoring. Lack of these may compromise an organisations ability to make decisions on the outsourcing services they receive, as well as manage the relationship with the outsourcing provider [Faile 2001].

Data and System Resource Integrity and Confidentiality

Appropriate levels of security should be provided to the data and system resources it uses by the outsourcing provider. As the outsourcing provider has access to an organisation's confidential information, it can be delivered to unauthorised parties, for illegal use or financial gain in some instances.

Service Problems

Organisational Expectations

Another challenge in security outsourcing is standard of service the organisation expects from its service provider and the service that is delivered, as organisations may be accustomed to a certain standard of performance provided by its in house IT department prior to outsourcing. This same standard may not be continued by the outsourcing provider. This extent of difference can be a point of conflict until both organisations grow accustomed to the new environment [CICA 2003]. Other issues that can cause conflict include operational priorities or other key expectations and failure to meet defined standards of performance quality.

Cost Problems

Unanticipated costs

When security outsourcing is not effectively planned, an organisation can acquire unexpected costs related to transition and management, which can affect the profitability of the outsourcing decision [CICA 2003]. The organisations and outsourcing provider's understanding of which services are included in the agreement and which represent additional chargeable services are often different. Some outsourcing providers may charge extra for services such as training or personal computer support. This makes cost determination difficult and uncertainty of the amount that will be charged.

Further than this, it may be difficult to compare the contracted costs of outsourcing security services, with what might have been incurred with in house operations. The lack of financial benchmarks allows inadequate financial performance to be unrecognised and not managed [CICA 2003].

MAKING AN OUTSOURCING DECISION

Once the organisation has decided to outsource its security, the first step is to determine exactly what will be outsourced and what applications will be kept in house. Organisations should research outsourcing providers and the services they provide as the outsourcing decision is one that should not be made lightly as it can have a significant influence on the reputation and the performance of the organisation. During this

time, the organisation evaluates the credentials of potential outsourcing providers to determine if they are able to meet their requirements [Faile 2001].

This should include research into the following issues:

Financial and Operational Interests

It is important to develop a thorough understanding of the outsourcing provider's financial and operating conditions as well as a review of the organisations processes before entering into an agreement. This review should examine the outsourcing provider's ability to meet the organisation's needs and objectives, and can include a review of financial records, meetings with management as well as on site visits [Faile 2001].

Experience and Expertise

Organisations must be careful in evaluating the outsourcing provider's experience and ability with the types of systems and applications to be used, as well as its ability to maintain the systems in operation and respond to service disruptions. Meeting with the outsourcing provider's staff and its other clients may aid in evaluating the provider's qualifications and experience and give an indication of their business culture [Faile 2001].

It is also important to examine the policies and procedures the outsourcing provider has in place relating to the protection of systems, data and software, and controls over security, IT recovery, systems development and maintenance. They should show adequate knowledge of laws and regulations relevant to the services they are providing to other organisations [Faile 2001].

Cost

It is important that organisations come up with several alternatives when researching the affordability of the services offered by outsourcing providers. Larger providers are often able to offer affordable prices due to their size. Whereas new security providers entering the market may also offer reasonable prices as they try to gain market share [Faile 2001].

Location

The location of providers can be an important factor as some mostly smaller providers, are limited geographically as to whom they are able to serve. Other larger providers can provide the means for their clients to connect into a central location where the outsourcing provider is able to monitor all of the networks it is responsible for, eliminating geography issues [Faile 2001].

Level of Comfort

Before agreement negotiations take place, an organisations management should visit outsourcing providers and meet the people who will be monitoring its networks as well as the management team. This provides an indication of the business culture of the provider and how they conduct business [Faile 2001].

Service Level Agreement

Once a suitable provider has been identified, contract negotiations can begin to be formalised. Specifically a Service Level Agreement (SLA) will be negotiated at this time. This contract identifies the scope of the service, fees, it can limit the amount of access the outsourcing provider has to an organisations sensitive information, establish roles and responsibilities during attacks, as well as establish a quantitative measure of the outsourcing providers performance [CICA 2003].

The following paragraphs give an overview of some of the issues that need to be addressed in the SLA:

Scope of Service

The scope of the service, its duration, renewal terms, and the rights and responsibilities of both organisations to the agreement should be clearly described as well as all relevant performance measures, fees and responsibilities for the services to be performed [CICA 2003].

Fees

The agreement should address the fees charged for services, the costs of purchasing and maintaining hardware and software, etc. Issues such as refunds and credits, disputed charges should also be addressed as well as duration, renewal terms, the right to raise fees, and limits on fee increases should also be specified [CICA 2003].

Performance Measurements

The purpose of this is to provide the client with some quantitative measure of the provider's performance that will ensure that the organisation's requirements are met [CICA 2003].

Termination

It is essential that both organisations define the circumstances under which they may terminate the agreement. Putting termination rights, terms and conditions into the agreement can provide acceptable options in problematic situations [CICA 2003].

ETHICAL CONSIDERATIONS

The following are examples of how the media have reported instances of fraud within Security Outsourcing operations:

CASE 1

On 9 April 2005, the cyber crime cell of police in Pune, India, arrested three former employees of an India based call center company, Mphasis, working in its Pune center, along with nine more accomplices, who they believed were involved in a fraud involving stealing money from five Citibank customers in the USA.

A day later, they announced that they have recovered US$23,000 (about 1 million Indian rupees). The investigations are still on and close to US$425,000 had been recovered. Apparently, the employees had obtained pins from the customers by talking to them on phone and then used that to create false accounts and transfer money from the victims account to their own [Das 2005].

CASE 2

India's booming outsourcing industry struggled with new political and security worries after a British tabloid reported that one of its reporters purchased private financial data on British citizens from an Indian outsourcing worker as part of a sting operation.

The Sun newspaper reported Thursday that a reporter posing as a businessman purchased the bank account details of 1,000 Britons -- including customers of some of Britain's best-known banks -- for about $5.50 each.

The worker who allegedly sold the information bragged to the undercover reporter that he could "sell as many as 200,000 account details a month" and declared that "technology is made by man and it can be broken by man," according to the newspaper. The Sun said the worker received the information from "a web of contacts who work in call centers."

The newspaper's report, which was widely covered in the Indian news media, has renewed criticism that outsourcing firms have failed to erect adequate protections against fraud in their zeal to take advantage of the booming demand from foreign companies seeking to lower costs by shifting some office operations abroad [Lancaster 2005].

The ethical issues relating to the media coverage of the cases are:

- Outsourcing is insecure
- Overseas outsourcing is insecure
- Low Security protection
- Staff working at Outsourcing centres are unethical

The problem with the media perception is that they cannot prove any of the facts that they have are stated.

CONCLUSION

As the Internet has become an integral means of conducting business, organisations are forced to find new ways to secure their assets. New technologies are increasingly complex, finding and retaining qualified security professionals and the difficulties associated with implementing technologies, it is very difficult to perform security properly. As a result security outsourcing is a rapidly emerging business [Faile 2001].

Security outsourcing providers can eliminate these challenges associated with training and retaining skilled personnel, as well as purchasing technologies and the regular upgrades associated with them. As a security provider, they should understand the fundamentals of defence-in-depth and be capable of deploying tools to assure this. The problem with recent cases reported in the media, is that they have been mis-reported what outsourcing is and have described out-sourcing as being unethical.

ACKNOWLEDGMENTS

The authors acknowledge the Australian Research Council and their funding for the project.

REFERENCES

[Aalders 2001] Aalders, R. 2001, "The IT Outsourcing Guide", Chichester, Willey.

[Burnett 1998] Burnett, R. 1998, "Outsourcing IT: the Legal Aspects", Aldershot, UK.

[CICA 2003] The Canadian Institute of Chartered Accountants, "Information technology Outsourcing", Toronto 2003

URL: http://www.cica.ca/multimedia/Download_Library/Research_Guidance/IT_Advisory_Committee/English/eIToutsourcing0204.pdf

Accessed: October 4, 2004

[Das 2005] Das S, 2005, A Tale of Two Frauds, Sunday, May 01, 2005
URL: http://www.globaloutsourcing.org/content/search/showarticle.asp?artid=72

Accessed: August 14th, 2005.

[Faile 2001] Faile, Jonathan S. "Security Outsourcing" GSEC Practical, 2001

URL: http://www.sans.org/rr/whitepapers/services/223.php

Accessed: October 14, 2004

[James and White 1996] James, B. and White, R. 1996 "The Outsourcing Manual", Aldershot, UK.

[Johnson 1997] Johnson, M. 1997, "Outsourcing – In Brief", Butterworth Heinemann, Oxford, UK.

[Lancaster 2005] Lancaster J, 2005, Outsourcing in India In Crisis Over Scam British Paper Alleges Security Breach, Washington Post Foreign Service Saturday, June 25,

URL:

http://www.washingtonpost.com/wp-dyn/content/article/2005/06/24/AR2005062401951.html

Accessed: August 14th, 2005.

Code of Ethics for Professionals of Information Systems - CEPIS

Helena Dulce Campos
Departamento de Sistemas de Informação, Universidade do Minho
Campus de Azurém
4800-058 Guimarães, Portugal
e-mail: helendoc@sapo.pt

Abstract

On the area of Technologies and Information Systems (TIS) there is a multiplicity of competences and knowledge. In order the professionals may carry them out with success and great advantage, the existence of a structured and standardized framework that could be used as a reference for any organization, is needed. Parallel to this problematic there still exists the acknowledgement of the impossibility of a technological life without code of ethics.

Looking to the Portuguese situation related to professions, competences and code of ethics of the professionals of TIS, we could conclude that there does not exist such a standards. Therefore, the objective of this work is to develop a model - CEPIS - *Code of Ethics for Professionals of Information Systems* - that standardises the ethical behaviour of professionals of the TIS. To achieve this objective, we propose: (1) a pattern of organizational and operational competences and respective professional skills; (2) the principles and obligations of the professionals for each competence; (3) a code of ethics for each of the identified competences.

So, the work comprises: (1) The creation of a matrix that identifies and classifies a pattern of competences – organizational and operational – and respective aptitudes and levels of professional responsibilities; adjusting to the respective importance that the TSI have in the organizations, and always aiming at the technological and methodological evolutions.

(2) Identified the main competences and aptitudes of the professionals of the TSI, it also have to be identified the fundamental ethical principals, in order to achieve their better performance. In a first analyse, these principals will include generic moral imperatives,

more specific professional responsibilities in the performance of the profession, imperatives of organizational leadership and the biggest conformity possible.

As a result of this work, it must be achieved a proposal for a code of ethics consisting of two parts:

1- The principle fundamental ethics, immutable in time and place, that is found above all philosophical and political concept and who are equal in any profession.
2- On the performing of each profession the principle specific ethics can vary in time and place.

(3) In order to observe if there exists the concern and practice of ethical professional attitudes at an academic and organizational level, a fieldwork will be developed.

For us, the term *professionals* not only include academicals, professionals, researchers, executives and consulters but also students of the TSI area (who will be the professionals of the near future). So the fieldwork will be split into two great sides: the academic and the organizational.

On the academic side, the work to be developed consists of an analysis of how a course in particular (Degree or MBA) prevents on their curriculum an ethical formation of their students. Namely, if there exists ethical disciplines that identify aspects that leads to ethical behaviours and preoccupations; that prepares them to deal with ethical questions; that alerts them for what kind of ethical behaviour is acceptable or not and that encourage them for better practices.

On the organizational side, to give an answer to one of the key problems referred on the development of the code (the fact that the validation of the individuals who were going to be influenced by the code completely is apart), we proceed with the fieldwork that will consist on the application of the proposed CEPSI model, in the different organizations and areas and that possesses a TSI department, hoping to obtain as a final result the validation and the contribution of the model in the enrichment and improvement of the performance of the professionals in the TSI communities. The great finality would be that the own TSI professionals will test the proposed model in order to be valid empirically.

On the application of the code it is necessary to have in mind the own requirements of each organisation, the respective individual competences attributed to their professionals; their culture; their mission; Their tradition; their strategic vision; their history; their dimension; their image and their market, i.e. the context were it is inserted. So, possibly there will be found surprises and even interesting establishments.

COPYRIGHT