Conference Proceedings of

AiCE 2002

SYDNEY, September 30th, 2002.

Third AUSTRALIAN INSTITUTE OF COMPUTER ETHICS CONFERENCE

Computer Ethics: Its impact upon Australia

Edited by:
Matthew Warren and John Barlow
ISBN 0 7300 2560 8
Proceedings of

AiCE 2002

Edited by
Matthew Warren and John Barlow
ISBN 0 7300 2560 8

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

All papers published in the conference proceedings have been blind refereed by at least two of the AiCE 2002 Program committee or reviewing committee.

© Australian Institute of Computer Ethics, 2002.
Welcome

The AiCE2002 conference follows on from the highly successful initial AICEC99 and AICE2000 conference. This conference looks at the continued development of Computer Ethics within Australia, papers covering issues such as: the teaching of computer ethics, security and ethics; the impact of computer ethics and the role of organizations.

Members of the conference review 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 review 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 with the start of the new millennium.

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

AiCE 2002 Organising Committee
John Barlow, Australian Catholic University, (Conference Chair).
Matt Warren, Deakin University.
John Weckert, Charles Sturt University.

AiCE 2002 Reviewers
Helen Armstrong, Curtin University of Technology.
John Barlow, Australian Catholic University.
Jo Coldwell, Deakin University.
William Hutchinson, Edith Cowan University.
Shona Leitch, Deakin University.
Craig Valli, Edith Cowan University.
Matt Warren, Deakin University.
John Weckert, Charles Sturt University.

AiCE 2002 acknowledges the support of:
Australian Catholic University
Charles Sturt University
## Contents

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security in Home Healthcare: A Case Study</td>
<td>6</td>
</tr>
<tr>
<td>R.ÄHLFELDT</td>
<td></td>
</tr>
<tr>
<td>Character and the Internet</td>
<td>16</td>
</tr>
<tr>
<td>S.CLARKE</td>
<td></td>
</tr>
<tr>
<td>Watching your own: The problem of insider IT misuse</td>
<td>22</td>
</tr>
<tr>
<td>S.FURNELL AND A.PHYO</td>
<td></td>
</tr>
<tr>
<td>Information Privacy and Data Quality: The Problem of Database Fragmentation</td>
<td>30</td>
</tr>
<tr>
<td>M.GIBBS</td>
<td></td>
</tr>
<tr>
<td>Ethical and Privacy Issues in Genetic Databases</td>
<td>39</td>
</tr>
<tr>
<td>H.GIGGINS AND L.BRANKOVIC</td>
<td></td>
</tr>
<tr>
<td>Ethical Issues for Professional Web and Software Designers: Are there 2 classes of users?</td>
<td>51</td>
</tr>
<tr>
<td>B.HARDY AND O.BURMEISTER</td>
<td></td>
</tr>
<tr>
<td>Internet Banking: Security, Ethics and Trust</td>
<td>57</td>
</tr>
<tr>
<td>D.HUTCHINSON AND M.WARREN</td>
<td></td>
</tr>
<tr>
<td>Privacy Protection – Can we afford to Wait?</td>
<td>68</td>
</tr>
<tr>
<td>G. KING-SIEM AND I. MORRISON</td>
<td></td>
</tr>
<tr>
<td>Designing Ethical Systems for Electronic Commerce</td>
<td>73</td>
</tr>
<tr>
<td>S.LEITCH AND M.WARREN</td>
<td></td>
</tr>
<tr>
<td>Workplace email: surveillance, privacy and ethical protocols</td>
<td>80</td>
</tr>
<tr>
<td>P.ROBERTS</td>
<td></td>
</tr>
<tr>
<td>The Inadequacy of Existing Ethical Codes for On-line Research : A matter of Informed Consent</td>
<td>88</td>
</tr>
<tr>
<td>P.ROBERTS AND J.WEBBER</td>
<td></td>
</tr>
<tr>
<td>The Effectiveness of the Co-Regulatory Scheme for Internet Content Regulation</td>
<td>96</td>
</tr>
<tr>
<td>G.SANDY</td>
<td></td>
</tr>
<tr>
<td>Accessible E-Commerce: Crossing the digital generation gap</td>
<td>106</td>
</tr>
<tr>
<td>H.SCOTT, O.BURMEISTER AND S.ROBERTS</td>
<td></td>
</tr>
<tr>
<td>Doing Ethics: a universal technique in an accessibility context</td>
<td>118</td>
</tr>
<tr>
<td>C.SIMPSON, L.NEVILE AND O.BURMEISTER</td>
<td></td>
</tr>
<tr>
<td>Killer Robots</td>
<td>128</td>
</tr>
<tr>
<td>R.SPARROW</td>
<td></td>
</tr>
</tbody>
</table>
An Examination Of Non-Business Usage of the World Wide Web in Two Western Australian Organisations  
C.VALLI  

130

Australian Hackers: an Ethical Perspective  
M.J.WARREN AND W.HUTCHINSON  

139

Reflections on the Australian Computer Society Code of Ethics  
S. L. WHEELER  

148
Information Security in Home Healthcare: A Case Study

Rose Mharie Åhlfeldt

Department of Computer Science, University of Skövde, P.O. Box 408, S-541 28 Skövde, SWEDEN

Email: rose-mharie.ahlfeldt@ida.his.se

Abstract

Home healthcare is an expanding research area and it has become necessary for municipalities to manage medical information with the same confidentiality as with other care performers. Patient-related information stored in healthcare organizations is defined as sensitive information, and must be managed at a high security level. This paper reports on experiences from a case study in two municipalities in the region “Västra Götaland” in the southwest of Sweden. One of the municipalities has a manual system and the other has a computerized system for personal data management. The research is based on the recommendations and common advice for processing of personal data compiled by the Data Inspection Board in Sweden. The case study points out three main deficiencies in the area of information security in home healthcare regarding personal integrity and secrecy: 1) It shows the necessity of a clear need for security training among personnel involved in home healthcare. 2) It also shows the need for elaborate security measures, including levels on access profiles in the computerized system. 3) The heavy use of facsimile transmission for information distribution is another weak point concerning security.

Keywords: Information security, home healthcare, healthcare informatics, personal integrity, secrecy

Introduction

Healthcare is an information-intensive organization, and a major part of the business includes the exchange of information. Therefore it is natural to use the support of computers in order to efficiently improve such an information-intensive organization. The increasing application of computers increases the accessibility of data, especially when modern techniques, such as a network of terminals directly coupled to computers and local area networks, are applied. Unauthorized use of the data is not an illusory danger. Therefore, the access to these data must be regulated. The fact that not everybody has access to the data is a logical consequence of the right to privacy. The individual must be able to check what have been registered about him or her and to whom data are distributed. Therefore, laws to protect privacy have been introduced and information security in healthcare proceeds from laws, practice and ethics [1].

Healthcare in Sweden is performed by county councils, municipalities and private care performers. The Swedish reform “Ädelreformen”, which came into force in the turn of the year 1991/1992, has transferred the main part of home healthcare to the municipalities. The municipalities have gotten liability for all care, except for medical
efforts performed by physicians. Therefore, there is never a complete care team in home healthcare. Instead many organizations participate [2].

In 1998, the Data Inspection Board publishes a report about processing of personal data in hospitals [3]. In this report they pointed out that carefulness of the patient’s integrity and protecting the secrecy are a foundational view in healthcare. This view seems to be more important when data is computerized. They also considered defective management of patient’s data in the computerized area.

Irrespectively of if the data is computerized or not, the case study investigates home healthcare in order to examine if it has the same defective management of patient’s data as the Data Inspection Board has identified in hospitals [4].

The case study includes observations and interviews in two municipalities in the region “Västra Götaland” in the southwest of Sweden.

The aim of this paper is to present the results and discussions from the case study of information security in home healthcare regarding personal integrity and secrecy. A brief description of information security in healthcare is given in section 2. Section 3 describes the research approach. The result of the observations and interviews is presented in section 4 and discussed in section 5. Finally, a conclusion and possible future research is presented in section 6.

**Information Security in Healthcare**

Information Security is a concept that is difficult to define even for those people working within healthcare. Information in different forms is a necessity for the healthcare work, and security is an obvious requirement for almost everything anyone does in healthcare. Irrespectively of if it is a computerized or a non-computerized system that is handling the information in healthcare, the information demands should be the same.

There is some related work going on in the area of information security in healthcare. SITHS¹ (Secure IT within Healthcare) is a Swedish project with the aim to develop models and methods to realize the basic security functions of IT-support in healthcare. These basic functions are:

- **authentication** – control of the given identity
- allocation of **authority** – determination of the access rights
- **secrecy** – protection of information against improper insight
- **integrity** – protection of information against undesired changes, influences or insight
- functions for **traceability** – possibilities to trace actions and events to a specific user and in this way keep proper users responsible for their actions.

¹ SITHS – a Swedish acronym for “Secure IT within Healthcare”
## Information security

<table>
<thead>
<tr>
<th>Traceability</th>
<th>Integrity</th>
<th>Secrecy</th>
<th>Accessibility</th>
<th>H-secrecy</th>
<th>Administration security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinctly derive performed operations to an individual.</td>
<td>Protection against undesired changes.</td>
<td>Data must not be accessible or unveiled to unauthorized people.</td>
<td>To use resources as required in expected extension and within desired time.</td>
<td>System security</td>
<td>Communication security</td>
</tr>
<tr>
<td>Security that information is obtained with help from related administrated resources.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-repudiation</th>
<th>Authentication</th>
<th>Authority</th>
<th>Connect security with transmission of information or steering signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>A reception or dispatch of a message can never be denied.</td>
<td>Control of given identity.</td>
<td>The user’s right to use resources in the system</td>
<td></td>
</tr>
</tbody>
</table>

### Table 1. Information security [7]

SITHS defined information security as the collected effect of measures to minimize the risks intended for the accessibility, secrecy, integrity and traceability of information [5]. The SITHS-project has presented a summary of the basic functions, (see Table 1).

Dahlin & Arnesjö [6] use data security as a security concept for computerized patient records. To say that a patient’s record has data security some issues are required:

- data does not get lost
- data can not fall into the wrong hands
- data is available when needed
- data is reliable

An important element in the information security area is the awareness of the importance of data protection within the organization. Van Bemmel & Musen mean that activities are necessary to make the members of an organization aware of the importance of data protection [1]. The introduction of computers in healthcare has also increased people’s fears that their private life will be jeopardized. A registered person must be able to check what has been registered about him/her and to whom data has been distributed [1]. The SITHS-project also mentions two models to access information in a computerized system, the authority model and the logging model [5]. The authority model implies that a user’s access to information is totally managed in advance by the regulated acquisition. The logging model implies that a user has full access to information on his/her own responsibility and all measures can be checked afterwards. The SITHS-project recommends a combination of the two models. The reason is that an isolated logging model runs the risk of minimizing the trustworthiness for the information handling in healthcare, while an isolated authority model probably is overthrown because of the extensive administration this model is required, (see Figure 1).
Secrecy is another important element in the area of information security. The nursing staff has normally an instinctive feeling about that sensitive information always must be protected against observation, against improper access and against manipulation possibilities. At the same time there is an uncertainty among the healthcare staff about the limits allowed in the performed information handling. This uncertainty has been strengthened by the introduction of IT in healthcare and by new legislation\(^2\), which has not yet gotten its full interpretation and application.

In its third report, the SITHS project declares that the most important element for how to make information security work in an optimal way is education [11]. It is in education that existing threats, risks and possibilities can be pointed out. The SITHS-group proclaims that this is the way to build security awareness. Measures of security, no matter how technically advanced they are, can never replace the knowledge of the staff and their attitude to the security work. Furthermore, it is enormously important that ethics and moral is kept on a high level so the trustworthiness for healthcare is enforced [11].

To reach good information security, it is not enough with only security functions and technology in the system. Also, a structured way of working for the security work as a whole is required. The work must be impelled as a continuing process from the demands of the business to build up and maintain a conscious and adapted level of the information security [5].

\(^2\) The Act on Healthcare Record and The Personal Data Act
Research approach

The Data Inspection Board points out in their report that the computerization of Swedish healthcare is widespread [3]. In spite of healthcare by tradition being very anxious about the patient’s integrity and defending their secrecy, there are still deficiencies in the management of the patients’ healthcare data in computerized systems. The examinations of the Data Inspection Board have been intended for the hospitals where the county councils are the responsible authorities. The research described in this paper has a focus on home healthcare with the municipalities as the responsible authority.

According to the recommendations by the Data Inspection Board, following questions are asked:

- How is the patient’s identity checked?
- What strategies exist to ensure that the strict information requirements enforcing by the act are adhered to?
- How are the constitutions and other organizational rules distributed to the staff to ensure that the proper statues are followed?
- How is unauthorized access prevented in patient records? What are the needs to improve the protection against unauthorized access in existing and future systems?
- Are there any clearly distinguished levels of access? Are there any persons in charge keeping the authorities up-to-date?
- Are there any routines for following-up the information security in the organization?
- Is there any existing educational programme in the organization in order to educate the healthcare staff in information security policy?
- Is sensitive information in the system logged? How is the log checked and managed?

The work was done in the form of interviews with the responsible persons and the healthcare staff working in home healthcare. Also a field study was conducted to get a relevant idea of how the management of the personal data works by following the healthcare staff in their work.

Two municipalities were chosen, one with a computerized system and one with non-computerized system. Three persons from each municipality were observed, district nurses, staff nurses and nurse’s aids. After the observations, the observed people have the opportunity to read through the text. The aim was not to give the observed people the opportunity to change something, but instead to inform them about the results and to make sure that there were no misunderstandings. The interviewed persons were the observed people. Furthermore, two unit manager and two medical responsible nurses were also interviewed. In total, ten persons, five from each municipality.

The interviews were performed in a discussion form. The interviewed persons did not see the questions before the interviews. The interviewer asked the questions and the interviewed persons did answer to best of their ability and the answers were written
down. The notes were then rewritten and sent to the interviewed persons for validation.

Results

It should be pointed out that the basic strategies for the information security, especially the IT-strategies, are worse in the municipalities than in the county councils. Both municipalities included in this work, have deficient IT-strategies. In one of the municipalities it has been impossible to have access to any IT-strategies. According to reports, there exist old strategies that are not relevant anymore. New IT-strategies are in process but not yet accessible. In the other municipality, there is a proposal presented to the Municipal Executive Board about developed IT-strategies, but these are very general and are more on an all-embracing level, far away from practical guidance for the users who use the systems in the daily work.

Whether the systems are intended for care or not, the basic strategies for managing the systems are deficient or not even existing. This implies that there are already deficiencies in the information security on a basic level. Strategies must exist for basic functions like back-up routines, virus protection, cryptographic techniques, fire security etc.

From the result of the observations and interviews, three main points could be held up as apparent deficiencies in the information security [8 and 9]. These points are: education, levels on access profiles and facsimile transmissions as information distributor. These three points are described in more detail in following subsections.

Education

There is no specific educational programme for information security in either of the two municipalities. The municipality with a non-computerized system has the intention to soon introduce a computerized system and they are delighted to include education in security in the ordinary educational programme. However, today it is not in the educational plan. The municipality with the computerized system had not either any specific educational program for information security. In the education of the computerized system, some questions of security arose in the context of user names, passwords etc., but regarding the staff it was more common that the users themselves ask these questions than it was included in the educational programme.

Furthermore, for both systems, none of the interviewed persons can see that there are any routines for following-up and evaluating the information security. There is no evaluation or following-up about how the information security is managed according to the staff.

Levels on the access profiles

In both investigated municipalities, there are levels of authorities between the part of the record standing by the HSL\(^3\) and the part standing by SOL\(^4\). They consider that

---

\(^3\) HSL - a Swedish acronym for the Act of Healthcare

\(^4\) SOL - a Swedish acronym for the Act of Social Service
these levels of authorities are satisfactory. In the computerized system, on the other hand, there are no differences in the levels of authorities between the occupational groups in the part of record standing by the HSL. The nurses have access to e.g. the whole records of the occupational therapist and vice versa. The levels of authorities are under consideration and the largest problem in this context is the administration of the authorities. It is the responsible person of the system who is in charge of up-dating the authorities, and the staff’s experience is that it is satisfactory. It is a greater problem that there are new employees with no user names than there is a problem with too old user names in the systems. Deputies and employees by the hours generate a larger amount of administration of authorities and lead to problems in computerized systems.

In this work, the computerized system has practiced the logging model, which implies that all nurses have got the same access to all care-receiver records in the municipality irrespectively of which unit they are working in.

**Facsimile as information distributor**

During the observation the question about facsimile as an information distributor emerged. Personal data from the municipalities to institutional care is in most cases transformed by a written document sent with the patient. The transformation, occurring from the institutional care to the municipality or the primary care is mostly performed by facsimile transmissions. In some cases, some documents are transformed by the patients themselves or by mail. In both municipalities investigated, these documents are very often transformed by facsimile in a common way without any encryption.

The staff in both municipalities has a feeling that the facsimiles are not encrypted and here all personnel groups mean that there are lacks. There exist many transactions of sensitive information by facsimiles and it would be unfortunately if this information got in wrong hands. There are guidelines introduced such as give a call back at such a sensitive information transforming exists, but this requirement does not ensure the information is transformed to the right receiver. If the information has gone astray, it is already too late to do something about it.

**Discussion**

**Comparison between the manual and the computerized patient record system**

The difference between a manual system and a computerized system regarding information security is that the risk for deficiencies in the information security increases in connection with computerizing the patient record system. In the computerized system, all nurses have access to the care-receiver records in the whole municipality, which implies that the risk for internal unauthorized access increases. In the manual system, it is only the district nurse who has got access to the care-receivers’ records. For this reason the records are not available for other care-performers, why spreading of care-receiver records to other places is not any problem. Furthermore, it implies that the records are always locked up in the district nurse expedition where no other has entrance at which the risk for internal unauthorized access is reduced.
The disadvantage with the manual patient record system is on one hand; it can be hard to have the patient record accessible when it is needed but also, the patient record can be accessible both for external and internal unauthorized access. This research has shown that the risk for external unauthorized access is not big, neither for the manual system nor the computerized system. On the other hand, there is always a risk for internal unauthorized access.

**Education**

Concerning education of information security, there are no direct advantages that will be reflected in the budget. Here there is another set of values than clearly economical, which must be observed in the first place. If it is hard to reserve resources for education when economical gain advantages can be obtained, the question must be asked how important it is to provide education in information security, which can not directly give such advantages. When the personal integrity and protection of defending the secrecy are emphasized as an important part of the education, there are great risks not to give necessary allotments of the resources for this purpose, despite the legislation being clearly defined in this question and despite many recommendations and common advice existing to realize the security routines in the business.

The need is not on the first hand how the system can give support to the users. It is a greater need of resources at a higher level so there are opportunities to education for the users, partly to learn the systems but also education in information security and security awareness in general. These needs are not dependent on technique but of course the techniques can be used to mediate information to the users about current acts and directions, for example.

This work has pointed out that education has clearly fallen short regarding information security in both the computerized and non-computerized system.

**Levels on the access profiles**

As considered before, the computerized system has practiced the logging model. According to the SITHS-project, it is important for this kind of method that there exist systems and administration to follow-up the logs [7].

The principal aim is to develop and implement need-to-know access-controls that would protect patients’ healthcare data. The user would only be allowed to access information necessary to complete his or her job [12]. This is also associated with The Act of Secrecy.

The risk with the logging model is proclaimed to be obvious, which has also been shown in this work. The logging model is used to give all the users access on their own responsibility while, in lacks of resources, there are still no routines for checking the log file. The computerized system has got their record system for more than two years. However, during the first year the log has only been checked two times [9]. Considering the sensitiveness of the information managed in patient record systems, the access model is to prefer despite the amount of administration it requires. Perhaps the best practice would be to have a combination of the both models.
The levels of access in the system should be on a level, which gives the users confidence when using the system. It should not be the user’s responsibility to decide what information the user has access to. Today, the technique has the opportunity to give satisfactory support to the users, but then it needs to be implemented in the systems. The routines that administrate the authorities should be revised. Besides, the administration should be analyzed how it can be delegated out into the organisation.

**Facsimile as information distributor**

According to the transformation of information by the facsimile, these deficiencies can be measured effectively by consciously realising the risks which this kind of transforming lead to. If the existing recommendations by The Data Inspection Board are accepted, a satisfactory information security can be performed when the facsimile transforms personal data [10].

**Conclusion and further research**

The aim of the case study was to survey the security problem concerning personal integrity and secrecy in systems managing personal data in home healthcare. The result of the work has shown that there are security problems like inadequate education in information security and deficiencies in the levels of access. In addition, the work has shown that transportation of information by facsimile is deficient.

Furthermore, it must be notified as there are no any clear IT strategies in the municipalities in order to get a foundation to build the information security on, the possibility to get sufficient information security is minimized.

The municipalities do not have any long experience of handling care information and have not kept up with the development of systems handling this information. Administration of authorities is a problem in the municipalities. There is a large turnover of employees and there are different categories of appointments with different geographical reach. It is unfortunate to choose a more open strategy for authorities only because the administration of the authorities is a burden. This is not a problem only for the systems of care. The administration problem of authorities also concerns information systems in general.

One interesting future research aspect would be to find out in what way the administration of authorities can be facilitated. We must not come to the situation that we build computerized systems to facilitate the ordinary administration and then come to another form of administration, almost with the same burden and performed in a manual way. There should be opportunities to see if the allotment of the authorities could be delegated out into the organisation so it will not be so heavy to only a few persons. Furthermore, the administration of the authorities should be automated with the help of computer support in order to increase the capacity of the administration.

Security is an important part of the protection of the personal integrity. A satisfying security is a demand according to The Personal Data Act. Security is not something extra. Security is a normal part of doing business.
References


Character and the Internet

Steve Clarke,
Centre for Applied Philosophy and Public Ethics,
Charles Sturt University

Email: Stclarke@csu.edu.au

Abstract

Can we make reliable inferences about the character of people we interact with on the internet? An answer to this question is problematised by the work of Ross and Nisbett (1991) and other social psychologists, who argue that the vast majority of our ascriptions of personality traits are unreliable. More recently, arguments have been mounted in social psychology for the conclusion that we can adopt strategies to improve the reliability of our judgments of personality. However, the mediation of the internet may limit the viability of such strategies, in ways that I explore here.

Keywords: Attribution, Character, Cross-situational consistency, Fundamental attribution error, Internet

Introduction

We form opinions about the character, or personality, of the people we interact with and observe. X is courageous, Y is dishonest and so on. Lay judgements of personality are studied by social and personality psychologists. According to proponents of situationism, a longstanding and influential tradition in social psychology, we are prone to overestimate the importance and reliability of character attributions in the explanation and prediction of behaviour. Situationists also maintain that we are prone to underestimate the importance of the situations that people find themselves in, in the explanation and prediction of behaviour.

Situationism comes in degrees. In the 1970s and 1980s social psychology was captivated by an argument due to Lee Ross (1977), in favour of a very extreme form of situationism which involved scepticism about the accuracy of virtually all of our judgements of personality. Ross’s (1977) defence of extreme situationism is reprised in the well-known book ‘The Person and the Situation’ (Ross and Nisbett 1991) According to Ross (1977) and Ross and Nisbett (1991) lay judgements of personality typically involve the commission of a ‘fundamental attribution error.’ (FAE), also known as ‘correspondence bias’. In the last ten years there has been a trend away from extreme situationism in social psychology. Even the staunchest defenders of extreme situationism, such as Ross, are now having second thoughts (Ross 2001).

One of the reasons for this is that social psychologists have come to appreciate that there are ways in which we act to mitigate the effect of the FAE. Nowadays social psychologists are generally more circumspect about making broad generalisations about our abilities at ‘person perception’. Nevertheless, there may be significant classes of circumstances in which we do persistently fall into error, mis-attributing
behaviour to peoples’ personalities, when, in actual fact, it is substantially the product of the situations in which those people are to be found.

For most of us the internet is a very recent addition to our lives that enables us to communicate with more people, more easily than we were able to previously. The internet offers us a variety of modes of communication, but by far the most common is the exchange of text-based email messages. I am in contact with dozens of people who I know of only through email communication; and I am anything but unique in having so many internet-only correspondents. Sometimes, like others, I form assessments of people’s characters on the basis of the information they provide to me in their email messages. Short abrupt messages suggest a cold personality; frequent spelling mistakes and punctuation errors suggest a careless personality, and so on. How reliable are these sorts of character assessments? I’m going to argue that they are very unreliable; far more unreliable than ordinary judgments about the characters of people that we interact with face to face. To present the argument we will need to go over debates about the FAE in social psychology in somewhat more detail.

If I am right about the unreliability of character assessments on the internet, then there are important ethical consequences that follow. The concept of character underpins two very important ethical concepts, responsibility and virtue. Virtues and vices are character traits, on most accounts (Doris 1998), so if we cannot reliably attribute character traits then we cannot reliably attribute virtues and vices. A correspondent who sends abusive messages to us may appear to be vicious and vulgar, but we should refrain from making any firm judgements about their character. If characters are not the primary causes of particular instances of behaviour, then there is a strong case to be made for the claim that we are not responsible for those particular instances of behaviour. Suppose that someone holds a gun to my head and forces me to scrawl graffiti on a wall, on pain of death. In such circumstances we would want to say that I am not responsible for the graffiti. The situational factor of having a gun against my head caused me to graffiti the wall and it was not an outcome intended by me. In general, if our behaviour is situationally caused and not a product of our intended activity, then we are not held to be responsible for its occurrence. If we cannot reliably attribute character to the behaviour of those whom we interact with via email because we have reason to believe that their behaviour is situationally caused, then it looks like we should not attribute responsibility either.

**The Fundamental Attribution Error**

According to social psychologists we explain behaviour by appealing to a combination of situation and personality. Generally, we assume that personality traits will exhibit considerable ‘cross-situational consistency’ (CSC). To say that someone is tidy is to make rough predictions about her behaviour in a variety of different situations. If we believe that someone is tidy, then we tend also to believe that her office is tidy, her car is tidy, her clothes are tidy and so on. This is where we go wrong, according to situationists, who argue that we are perennially mistaken about character claims, precisely because we are apt to assume much more CSC than we are entitled to assume. If we observe that a colleague has a tidy office we will be mostly right in predicting that she will continue to maintain a tidy office. However, we will be quite likely to be wrong in assuming that she also has a tidy house or car. We
might avoid this problem by only attributing the trait of being ‘tidy in the office’ to our colleague. However, most lay character attribution doesn’t involve any such situational qualification and therefore involves us committing the FAE, according to Ross (1977) and a host of other situationists.

Evidence for the FAE is provided by a number of experiments (Ross 1977). Needless to say, not everyone agrees with the interpretation of these experiments that has it that there is an FAE (Funder 1995, Sabatini et al. 2001). Nevertheless, this is the dominant interpretation of such experiments in social psychology. One striking experiment that has been taken to demonstrate the effect of the FAE is Darley and Batson (1973), also known as the Good Samaritan experiment. In this experiment, students at the Princeton Theological Seminary were asked to give presentations about the parable of the Good Samaritan at a prearranged time and place. Getting to the location of the presentation involved passing a doorway where a confederate of Darley and Batson (1973) was to be found, coughing and groaning, in apparent need of medical assistance. Good Samaritans, famously, help those in need and one might expect the vast majority of theologians on their way to give a presentation about the parable of the Good Samaritan to act like the Good Samaritan and stop and help. In fact 63% of the seminarians who were slightly early for the presentation stopped and helped. Amazingly though, only 10% of those who were running slightly late for the presentation offered any form of assistance. This low rate of assistance was observed despite the fact that there was no penalty for being late to the presentation and despite the fact that helping behaviour was construed in an extremely broad sense.

The Darley and Batson experiment (1973) might be taken to show that seminarians are callous and cruel and that our assumptions about them are wrong across the board. However there is no evidence that seminarians are consistently callous and cruel. 63% of seminarians act altruistically when they come across a stranger in need of assistance and are unhurried. Situationists argue that this experiment demonstrates that subtle changes in situation can have a profound effect on behaviour, in ways that generally go unrecognised. Further thought about the experiment highlights serious difficulties for our character attributions. We expect that, if the seminarians are disposed to be helpful, then they will be disposed to be helpful across a wide variety of situations. In making this assumption, based on the assumption of a high level of CSC in the expression of character, we are shown up. Behavioural expressions of character are not as cross-situationally consistent as we expect them to be. Furthermore, it seems that we are very bad at adjusting our practices of character attribution to accommodate these results. In a follow up study Pietromonaco and Nisbett (1982) had subjects read a summary of the results of Darley and Batson (1973) and then asked them to predict the results of a very similar study. Pietromonaco and Nisbett (1982) found that subjects made only insignificant adjustments to their preconceptions about the relative importance of character and about the relative importance of situations, as components of a proper explanation of behaviour in this study, despite having been informed of the striking results of Darley and Batson (1973).

**Ecological Validity**

Ross (1977) and Ross and Nisbett (1991) argued that the FAE was extremely pervasive. However other commentators have expressed doubts about its
pervasiveness on the grounds that the experiments that are used as a basis for the case for the FAE may lack ‘ecological validity’. Experiments conducted by situationist social psychologists identify circumstances in which our explanatory constructs are revealed to be insensitive to situational variation. However, those are the exact circumstances that situationist social psychologists look to, to support their case. In the words of Gilbert and Malone ‘Because no effort is made to select representative situations or subjects, such experiments cannot reveal the kinds of attributions people usually, normally, routinely, generally or typically make.’ (Gilbert and Malone 1995, p. 28).

There are a variety of other criticisms of the case for thinking that a pervasive FAE has ecological validity. The line of criticism that I want to focus on here is that we may be able to correct for the FAE if and when it occurs. In classic experiments exemplifying the occurrence of the FAE, subjects are asked to make one-off judgments about people’s personalities or their behaviour and are given no opportunity to correct those judgments. However, many of our judgments of character are not one-off judgments and many are subject to correction over time. In recent times multistage models of lay attribution have become very influential in social psychology (Trope and Gaunt 1999, Gilbert 1998). A common feature of such models is that they postulate that we make character assessments automatically and non-consciously. It is only when we notice discrepancies between our automatic judgements of character and behaviour that we make conscious corrections to those judgments.

Although correction of our lay judgements of character is not a taught form of behaviour there is evidence that we are very good at it. Trope and Bassock (1982) demonstrate that we are very good at formulating ‘diagnostic questions’, questions designed to elicit information about people that can both confirm and disconfirm hypotheses about character. Fein (1996) provides evidence that when we become suspicious of the motives of others our ability avoid errors of judgment is dramatically increased. Baron and Misovich (1993) point out that we can improve our judgements of character by creating circumstances that test people’s characters.

**The Internet**

Our ability to make reliable judgements about character is also an ability to make reliable judgements about the impact of situations on character. To know how a courageous person will behave is to know, roughly, how that person will behave, in a variety of different situations. We would not be surprised if a very courageous person ran away from an armed killer. However we would be extremely surprised if a person whom we thought of as courageous ran away from a barking chihuahua. In fact, we would probably be prompted to alter our opinion of them.

The main difficulty, as I see it, in making judgements of character about the people we interact with on the internet is that, typically, we have very little situational information to base our judgements on. When we observe people directly we are able to make reasonably accurate judgements about the situations that they are in. However, when we interact with them on the internet we have very little information about the situations that they are in. When I receive an email from a correspondent, it
may have been sent from a work situation, or from a home situation, or it may have been sent from an internet café whilst the correspondent was on holiday. Because I have very little information about their situation I cannot follow the usual procedure of adjusting my observations about their behaviour in light of situational facts in order to come to generalisations about their character. The case for the occurrence of a pervasive FAE depended on us being poor at noticing subtle changes of situation, but nevertheless making judgements about character. When we communicate with someone on the internet we are especially in danger of ignoring situational variations because we have little information available that might tell us what situation a person is in. So when we are communicating with someone via email, and make character judgements about them, we are especially prone to commit the FAE.

Might we be able to improve our judgments of others by employing the sort of strategies mentioned earlier to improve our judgments of others when we interact with them in a face-to-face mode? Unfortunately, the prospects for these kinds of improvements are not good. There is much more scope for people to manipulate the ways in which they are perceived by others on the internet than in face-to-face communication. Our inability to gain reliable information about people’s situations means that we cannot make corresponding reliable inferences about their characters. When someone asks me a ‘diagnostic question’ in face-to-face communication I am expected to respond more or less immediately. I can lie, of course, but I may not have time to craft a convincing lie and I run the risk of detection if my presentation is less than convincing, raising the prospect of further diagnostic questions. However, with email communication there is no expectation of an immediate reply, so the person I am asking a diagnostic question of has plenty of time to craft their reply. Furthermore, there are no cues from their body language to suggest that that I am being lied to. So there is very little that can prompt me to become suspicious of them, thereby enabling me to improve my judgement. Also, there is little I can do to create circumstances that test someone’s character, because I have little or no idea about the situation that they are in, in the first place. There are well-known cases where people have been able to use internet communication to deceive others about their age, their gender and their race. The internet makes such extreme forms of deception easy, in large part by denying people access to reliable situational information.

**Conclusion**

In summary then, because internet communication makes it particularly hard to make reliable inferences about the situations of our correspondents, we are particularly likely to overlook situational variations that will affect their behaviour. So, we are very vulnerable to committing the FAE when we make assessments of people’s character on the internet. There are a number of strategies that we can employ to overcome, or at least minimise, the effect of the FAE, but given the nature of internet communication it seems unlikely that these will be effective on the internet. The safest course of action, therefore, is to refrain from making character assessments about people whom we only communicate with via the internet. Our inability to reliably make character attributions has important ethical consequences. Once we forego character attribution to our internet correspondents, we will have to forego talk of their virtues and vices on the internet, as well as foregoing talk of their individual moral responsibility on the internet.
References


Watching your own: The problem of insider IT misuse

Steven Furnell and Aung Htike Phyo
Network Research Group, University of Plymouth, Plymouth, United Kingdom
Email: sfurnell@network-research-group.org

Abstract

In recent years the Internet connection has become a frequent point of attack for most organisations. However, the loss due to insider misuse is far greater than the loss due to external abuse. This paper focuses on the problem of insider misuse, the scale of it, and how it has effected the organisations. The paper also discusses why access controls alone cannot be used to address the problem, and proceeds to consider how techniques currently associated with Intrusion Detection Systems can potentially be applied for insider misuse detection. General guidelines for countermeasures against insider misuse are also provided to protect data and systems.

Keywords: Insider misuse; misuse detection; misuse countermeasures.

Introduction

If one was to play a game of word association and use the terms ‘security breach’ or ‘cybercrime’ as the starting point, it is very likely that words like ‘hacker’ or ‘virus’ would be amongst the first responses. It is somewhat less likely that terms like ‘employees’ or ‘insiders’ would emerge as many peoples’ first choices. In reality, however, insiders are very often the cause of the most significant and costly security incidents, and a significant proportion of what is commonly classed as cybercrime can be attributed to them. Indeed, the fact that insiders are already within the organisation often puts them in an ideal position to misuse a system if they are inclined to do so.

Although the great majority of the people are familiar with the generic meaning of the word 'misuse', when we try to map it to an IT context, there is a need to clarify certain issues. Insider IT misuse can be a very subjective term, and one of the most challenging tasks is to draw a clear line that separates an IT misuser from a person who is using a system in an acceptable way and for an approved purpose. The word ‘misuse’ implies the presence of rules that specify the conditions of allowable usage for the resources concerned. These rules are often embodied within an IT usage policy. However, such a policy, and hence the definition of misuse, can differ from one organisation to the other. For example, where some would give priority to detecting data-theft and unsanctioned modification of data, others might want to detect denial of services and Internet access abuse. Thus no single definition of misuse is appropriate for all organisations.

The aims of this paper are to present evidence of the insider misuse problem, and suggest possible means by which it could be addressed. The discussion begins by
examining the scale of the problem, based upon evidence from computer abuse surveys from recent years. This is followed by a more specific consideration of what can actually be considered to constitute IT misuse in an organisational context, which then leads into a discussion of methods that could potentially be employed to combat the problem.

The scale of the insider misuse problem

If one takes a look back to computer crime literature and surveys dating up to the mid-90s, the evidence presented would certainly suggest that the main threat was to be found from one’s own staff (with as much of 80% of computer crime believed to be the result of insider activity). In more recent years, however, many sources have indicated a significant rise in externally sourced incidents (principally in terms of Internet-based attacks such as website defacement and denial of service), with the consequence that although insider misuse is still significant, it now accounts for a far lesser proportion of raw incidents. For example, in the UK, results from the Department of Trade & Industry’s Information Security Breaches Survey 2002 revealed that only 34% of businesses considered their worst security incident to have been caused by an insider (DTI 2002). This possibly accounts for why 60% of respondents in the same survey were either not very concerned or not at all concerned about threats originating from their own employees. Hackers were the most feared threat, particularly amongst large businesses (with over 250 employees) where 50% expressed some level of concern about them). However, when considering the large businesses only, it should be noted that the split between those experiencing their worst incident as a result of internal staff versus external parties was almost equal.

Another source that has monitored the changing trend regarding internal and external attack is the annual CSI/FBI Computer Crime and Security Survey. Looking back to 1995, a key observation from the CSI was that “the greatest threat comes from inside your own organisation” (Power 1995). In more recent years, however, the survey results have painted a rather different picture, and by 2002 it was reported that, for the fifth year running, more respondents had cited their Internet connection as a frequent point of attack (74%), than had cited internal systems (33%) (Power 2002.). This may well be the case, but presenting the information in this manner tends to create something of a false impression, because the raw number of incidents is not necessarily the factor that we should be most concerned about. Of more interest to most CEOs, for example, will be the effect that the incidents had on their bottom line.

Many of the categories used in the CSI/FBI results encompass incidents that could potentially have been both internally and externally sourced (e.g. theft of proprietary information, sabotage of data networks, and virus). However, three of the categories very clearly indicate the source, and it is interesting to see the level of the annual losses that were associated in each case. The relevant information is presented in Table 1 (Power 2002). It is quite evident from the results that, although they relate to a five-year period over which the proportion of externally sourced incidents had exceeded internal ones, the quantifiable losses in the latter case dwarf those attributable to outside hackers. It is therefore clear that, in real terms, the level of the insider threat is still much greater than that exhibited by external hackers.
<table>
<thead>
<tr>
<th></th>
<th>System penetration by outsider</th>
<th>Inside abuse of Net access</th>
<th>Unauthorized insider access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>$1,637,000</td>
<td>$3,720,000</td>
<td>$50,565,000</td>
</tr>
<tr>
<td>1999</td>
<td>$2,885,000</td>
<td>$7,576,000</td>
<td>$3,567,000</td>
</tr>
<tr>
<td>2000</td>
<td>$7,104,000</td>
<td>$27,984,740</td>
<td>$22,554,500</td>
</tr>
<tr>
<td>2001</td>
<td>$19,066,600</td>
<td>$35,001,650</td>
<td>$6,064,000</td>
</tr>
<tr>
<td>2002</td>
<td>$13,055,000</td>
<td>$50,099,000</td>
<td>$4,503,000</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$43,747,600</strong></td>
<td><strong>$124,381,390</strong></td>
<td><strong>$87,253,500</strong></td>
</tr>
</tbody>
</table>

**Table 1 : Annual losses for selected incidents from CSI/FBI surveys**

The CSI figures relating to insider abuse of network access clearly suggest that, as well as bringing considerable advantages in terms of web and email communication, Internet access has also ushered in a whole range of new problems. This can be further evidenced by a survey of 544 human resources managers, conducted in 2002 and targeting large UK companies (with ‘large’ in this case being defined as those employing an average of 2,500 people). The results revealed that almost a quarter of them (23%) had felt obliged to dismiss employees in relation to Internet misconduct (with the vast majority of these cases – 69% - being linked to the downloading of pornographic materials) (Leyden, 2002). Many other cases resulted in less severe courses of action, such as verbal warnings or a discreet word in the ear of the person concerned, and in total the results indicated that 72% of respondents had encountered Internet misuse in some form.

**The nature of insider IT misuse**

One of the CSI/FBI categories from Table 1 was that of ‘unauthorised insider access’. However, one of the complicating aspects with insiders, and the aspect that differentiates this from the other insider category listed in the table, is that incidents will not always relate to something that is unauthorised. Indeed, the basic problem with insider misuse is that the person concerned has legitimate access to IT resources of the target organisation. This means that he/she does not need to bypass the authentication mechanisms of the IT infrastructure (no stealing or illegal reproduction of passwords and other forms of authentication tokens). Thus, in an IT context, insider misuse is the act of abusing granted privileges to cause harm. In this context, it can also be observed that users that know more about a system are more likely to abuse their privileges than users who are less knowledgeable.

Although this is not difficult to grasp, vagueness is introduced by the term misuse and what it means to different people or organisations. What is considered illegitimate use in one particular organisation can be perfectly acceptable for another. For example, browsing the web for personal use is outlawed entirely in some companies, whereas others are somewhat more relaxed about it and impose varying limits upon what is acceptable (e.g. some may permit up to 20 minutes per day, whereas others may allow twice this). In addition, there are myriad other activities that would likely be regarded as misuse in any organization, for example:
– Personal entertainment (e.g. playing games, writing personal email etc.)
– Downloading MP3s, pirated software, pornographic images, or other unsuitable material
– Fraud and theft (e.g. modifying payroll database to increase one’s wages)
– Sending out inappropriate material using company computers
– Installing and using pirated software.
– Reading or modifying another user’s files.

Although the computer security research community has created a plethora of taxonomies that describe computer intrusions in general (see Furnell et al. 2001 for an overview), little effort has been placed on the construction of a taxonomy that specialises in insider incidents. The earliest attempt to classify internal misuse of computer systems is presented by Anderson (1980) and discusses borders of distinction between masqueraders, clandestine users, and misfeasors. Masqueraders are insiders that exploit weaknesses of the authentication system, thus gaining the identity of other legitimate users. A clandestine user is related to authorised users and their capabilities to bypass audit, control and access resource mechanisms in a particular computer system. Finally, misfeasors are insiders who do not need to masquerade, but abuse the power of their privileges to misuse the system. However, as the small selection of examples above shows, the single category of ‘misfeaso’ can encompass a whole range of different incidents. As a result, other works have focused more specifically upon the issue of insider misuse, and indicative examples are given below:

– Tuglular (2000). This is the first comprehensive taxonomy of misfeaso incidents. The taxonomy classifies computer misuse incident in three dimensions: incidents, response and consequences. The entire taxonomy is orientated towards data collection for insider incident response.

– Magklaras and Furnell (2002). This taxonomy is human centric. Magklaras and Furnell perceived that all actions that constitute IT misuse lead back to human factors. The fundamental aspect for their taxonomy is classifying people in three basic dimensions: system role, reason of misuse and system consequences. This scheme is the most appropriate for threat prediction, but not suitable for detection.

Intentional misfeaso cases are performed for a variety of reasons. The best way to sub-divide them is to consider the motives in a way that could detect the ultimate goal of the abuser. It might be inferred, for example, that a legitimate user is trying to access sensitive data (data theft), take revenge against a particular person or an entire organisation (personal differences), cover indications of unprofessional behaviour, or deliberately ignore a particular regulation of the information security policy.

Unfortunately, despite evidence of the insider threat, there is no substantial effort devoted to addressing the problem of internal IT misuse. In fact, the great majority of misuse countermeasures address forms of abuse originating from external factors (i.e. the perceived threat from hackers). A significant reason for this is the difficulty in actually monitoring and detecting the problem in order to enable a response to be mounted. In the cases above, for example, it is clear that the misuse would have been
very difficult to control or prevent, as the perpetrators concerned were not violating any system-side access rules.

**Combating insider misuse**

The problem with insider abuse is that, once a user is authenticated to use a system, what he does with the system or the objects he has access rights to is neither monitored nor logged most of the time. Considering the list of potential misuses in the previous section, it is possible that appropriate access controls could be used to prevent some of them, but even these will not be sufficient for all contexts (consider, for instance, the case in which the misfeasor has legitimately been granted administrator level privileges). This epitomizes the difficulty in implementing access controls that resembles organisational hierarchy onto the IT systems. It must also be remembered that one user/process/account having all the privileges can lead to serious misuse by exploiting the situation. Neumann’s suggestion of multilevel systems and compartmentalization (Neumann 1999) should be given a serious consideration before we proceed with the insider misuse detection.

Today’s commercial operating systems are based on the old systems developed years ago. At the time when the core components of these systems were developed, the users were expected to behave themselves. The problem of insider misuse was not an issue. However the research in the IT security over the years has proved that people do misbehave and that insider misuse is a serious problem. Since these systems were not developed with insider misuse in mind, the preventive mechanism and the logging present in today’s commercial systems are not optimized for misuse detection. Existing access controls are not good enough to prevent insider misuse, making it more difficult to enforce insider misuse policies. For example, a user with administrator level privileges may not have the moral right to access confidential data on the system, but access controls present in today’s systems cannot prevent such actions. As such, it is considered that some form of supervision system is required to monitor for misuse activity.

Such technologies are already available to some extent in the form of Intrusion Detection Systems (IDS) (Amoroso 1999), but as with many other mainstream security technologies, these are geared towards detecting attacks on the system rather than misuse of it by legitimate users. Nonetheless, some of the principles are transferable. For example, current IDS employ two main strategies to identify attacks namely misuse-based detection and anomaly-based detection, and it is possible to see how each of these could be applied to the insider problem.

- **Misuse-based detection**
  In a traditional IDS, this approach relies upon knowing or predicting the intrusion scenario that the system is to detect. Intrusions are specified as attack signatures, which can then be matched to current activity using a rule-based approach. A similar approach could potentially be incorporated for misfeasor incidents, based upon those methods that employees have been known to exploit in the past, or those that they can be anticipated to attempt based upon the privileges and resources available to them. For example, at a conceptual level, one such misuse signature might relate to a user who is identified as attempting to modify a record about him/herself in a database.
(e.g. the payroll example indicated earlier). The principle here would be that, although their database privileges may allow them to do so, users should probably not be modifying details relating to themselves without someone else’s authority. Another example could be to watch for any sequence of events where a user accesses confidential information and then attaches it in an email destined for a recipient outside the organization. Neither of these rules would necessarily cause the user in question to be locked out of the system (because in some contexts the actions could still be quite legitimate), but they could be used to flag the activity for closer scrutiny.

– Anomaly-based detection

Rather than being based upon known or predicted patterns of misuse, this approach relies upon watching out for things that do not look normal when compared to typical user activity within the system. In a standard IDS, the principle is that any event that appears abnormal might be indicative of a security breach having occurred or being in progress. The assessment of abnormality is based upon a comparison of current activity against a historical profile of user (or system) behaviour that has been established over time. For example, past behaviour might suggest that a particular user typically downloads an average of 5MB of material from the web per week, and the nature of the attachments they assign to emails are normally documents. Therefore, if activity supervision detects a surge of download activity to 10MB in a single day, or a large number of email messages suddenly being sent with image attachments, then there would be reasonable grounds to investigate whether unsuitable activities might be in progress.

Although the above descriptions make the concepts sound relatively straightforward, it must be appreciated that neither technique can be considered 100% reliable, even in the context of traditional IDS. The consequence is that they can lead to false positives (where legitimate activity is believed to be intrusive) and false negatives (where genuine intrusive activities are misjudged as acceptable). The concept of applying the techniques for the detection of misfeasor activity / insider misuse makes the task more difficult, because we are dealing with legitimate users who are not violating access controls. From a misuse-based detection perspective, it is more difficult to identify the ways in which an insider might misuse the resources to which they have legitimate access, while from an anomaly detection perspective the level of behaviour profiling would need to be much more detailed and precise. When basing the assessment upon a comparison against their behaviour profile, a legitimate user misbehaving will almost certainly be more difficult to identify than a total impostor who is masquerading under the legitimate user’s identity. In addition, in an adaptive system, the process of profile refinement might be exploited by wily misfeasors who gradually train the system to accept misuse behavior as normal. As such, this aspect is still an area of active research, as the technical approaches are not mature.

When considering how to protect systems now, it is worth noting that preventative measures need not be technical. Security guidelines, such as the recommendations provided by the ISO 17799 standard (BSI 2001), typically suggest a number of personnel-related measures, which if employed correctly could dramatically reduce the likelihood of insider misuse being successful:
– Check references of prospective new employees before hiring them;
– Ensure that employment contracts include a clause relating to the acceptable use of IT resources;
– Ensure that adequate reminders about the ‘acceptable use’ policy are encountered by staff during their day to day use of systems;
– Ensure adequate supervision of staff by line management;
– Provide a means by which staff can confidentially report misuse of IT systems, without fear of recrimination from colleagues.
– Concerning the access of data, make sure that access control policies resemble organisation’s management hierarchy or rules.
– Security and access control policies need to be maintained to keep up with the change in organisation’s management hierarchy.

In the absence of an automated supervision approach, it would still fall to line managers and the like to enforce and monitor these aspects.

Conclusion

Insider misuse poses a great threat to organizations. Even though the Internet connection is the most frequent point of attack, the loss due to insider misuse is far greater than the loss due to external attacks.

At the present time, the system level countermeasures that can be implemented are limited. Current access control systems, although well-suited to guarding against unauthorized activities, cannot prevent insider misuse effectively if the subject is doing something within their legitimately assigned privileges. More advanced mechanisms, in terms of activity monitoring and supervision systems may offer a potential solution in the future. The authors’ ongoing research will design and evaluate approaches for realizing the latter approaches, and results will be detailed in future publications.

References


Information Privacy and Data Quality: The Problem of Database Fragmentation

Martin R. Gibbs

Department of Information Systems
The University of Melbourne, Australia
E-mail: mrgibbs@dis.unimelb.edu.au;

Abstract
The Privacy Amendment (Private Sector) Act 2000 has recently been enacted in Australia to regulate the way private sector organisations collect, store, use and disclose personal information. The ability of organisations to respond to the requirements of this new legislation is affected by the data quality of the personal information they hold. This paper examines one problem associated with data quality that erodes an organisation's ability to comply with the provisions of this new legislation: the fragmentation of customer data across multiple databases 'owned and operated' by separate function units within an organisation.

Keywords: Information Privacy, Data Quality, Australian Legislation

Introduction
Legislation to regulate the way private sector organisations handle personal information has recently been introduced in Australia. The Privacy Amendment (Private Sector) Act 2000 (Cth) (Private Sector Amendment) came into effect on the 21st of December 2001. The Private Sector Amendment applies to the vast majority of private sector organisations with annual turnovers of $3 million or more and to organizations that provide health services or hold health related information. It also applies to organisations with smaller annual turnovers that trade in personal information. The Private Sector Amendment regulates the ways in which these private sector organisations can collect, store, use and disclose personal information and it gives individuals the legal right to access and correct information held about them by private sector organisations (OFPC 2001a). As such, the Private Sector Amendment presents a number of challenges to organisations that collect, use and distribute personal information. In order to meet these challenges, many organisations will have to change the way they handle personal information.

The main repositories of personal information in most organisations are customer databases. Previous studies have shown that maintaining consistently high levels of customer data quality in these customer databases is a significant challenge and considerable expense for organisations (Redman 1998, Strong et al. 1997, Wang 1998). In this paper we argue that the ability of organisations to comply with the provisions of the Private Sector Amendment will be significantly compromised by the data quality of the personal information they hold. This connection between poor customer data quality and information privacy has not previously been explored in any detail yet is clearly important in determining an organisation's ability to comply with legislation designed to protect information privacy.
In this paper we report some key findings from an exploratory study designed to identify the significant issues created by poor customer data quality that face organizations as they adjust their business practices to meet the provisions of the new privacy legislation. The next section of this paper briefly describes the provisions of the Private Sector Amendment. Following this description we outline the connection between information privacy and the data quality of personal information. We then briefly describe our research approach before moving on to present and discuss some significant results from our study. In concluding this paper we observe that poor customer data quality erodes an organisation's ability to control the personal information it possesses. This erosion of control can seriously hamper an organisation's ability to comply with the provisions of the new legislation. Although the explicitly stated intention of the Private Sector Amendment is to 'give people some control over the way information about them is handled' (OFPC 2001b), this control cannot be secured by individuals unless organisation's have control of this personal information in the first place. Thus, poor data quality has significant implications for the protection of information privacy that extend beyond ensuring that personal information is complete, accurate and up-to-date.

The Privacy Amendment (Private Sector) Act 2000

Privacy is not a simple concept that can be easily defined. Most definitions of privacy invoke one or more of the following three key elements: anonymity, solitude and/or secrecy (See for example Johnson 2001 and Spinello 2000). These elements are often expressed as rights of the individual: the right to act anonymously, the right to live free of unwanted harassment, and the right for individuals to chose how they present themselves to others. When discussing privacy and information technologies, the last of these listed rights is often restated as the right for individuals to control the access others have to their personal information. Given that a number of possible definitions of privacy have common currency it is interesting to note that neither the Commonwealth Privacy Act 1988 (Cth) (Privacy Act) nor its more recent Private Sector Amendment explicitly define privacy. While privacy is not explicitly defined within these pieces of legislation, they do provide sets of 'privacy principles' for the protection of personal information. In addition, the Federal Privacy Commissioner has explicitly stated on numerous occasions that the goal of the Private Sector Amendment is to give individuals 'some control' over the personal information held about them by private sector organisations (FPC 2000, OFPC 2001a, 2001b). As such, it is useful to understand the definition of privacy implicit within the Privacy Act as pertaining solely to 'information privacy'. Roger Clarke (1999) has usefully defined information privacy in the following way:

Information privacy refers to the claims of individuals that data about themselves should generally not be available to other individuals and organisations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.

The Privacy Act regulates the way personal information is collected, stored, used and disclosed. Personal information is defined within the Privacy Act as:

Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or
not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. (The Privacy Act 1988 (Cth), Sect 6)

The Private Sector Amendments established ten National Privacy Principles (NPPs) as the minimum standard for information privacy in the private sector. The NPPs govern how an organisation should handle personal information. They cover: collection (NPP1); use and disclosure (NPP2); data quality (NPP3); data security (NPP4); openness (NPP5); access and correction (NPP6); use of government identifiers (NPP7); anonymity (NPP8); transborder data flows (NPP9); and sensitive information (NPP10).

The Private Sector Amendment is one of several recent measures introduced by the Australian Government to facilitate Australia's transition to an information economy (DCITA 2000). The new provisions have been implemented with the stated aim of balancing individual's rights for information privacy against the 'right of government and business to achieve their objectives in an efficient way' (FPC 2000, 2). In the spirit of promoting a 'culture that respects privacy' (FPC 2000, 2), privacy has been promoted as being 'good business' (OFPC 2001c) as well as being good for individuals. In particular, the legislation has been implemented with the recognition that consumers' lack of trust in the way commercial organisations handle their personal information is a major barrier to the growth of e-commerce (OFPC 2001c). The legislation also represents an attempt to bring Australia into line with international privacy regimes especially those of the European Union (EU) given the possibility that the EU will impose trade restrictions on nations that do not adequately protect the personal information of EU citizens.

In developing the provisions of the Private Sector Amendment the Australian government has deliberately opted for a 'light-touch' co-regulatory approach to the regulation of privacy with the aim of encouraging compliance through facilitation rather than through the threat of punitive actions for non-compliance (OFPC 2001d, 2001e). This approach has been designed to minimise the burden of compliance for businesses. It is also an approach that has attracted strong criticism and has led to the amendments being dubbed 'anti-privacy laws' (Roger Clarke quoted in Haslam and Mitchell 2001) and described as 'reducing existing privacy protection' (Clarke 2000) due to the large number of exceptions and qualifications built into the legislation and because it seemingly 'legitimises many unreasonable uses of personal data' (Clarke 2000). The legislation has also be criticised for lacking in 'grunt' and being 'toothless' due to the Federal Privacy Commissioner not being granted significant investigative powers or an ability to impose significant punitive penalties for breaches of the Privacy Act (McClelland in Australia, House of Representatives 2000, 22233-7). While these criticisms are significant and have a significant bearing on how private sector organizations have responded to the new privacy provisions, they are not the major focus of this paper. Rather, we wish to discuss the unexplored issues associated with how poor data quality in personal information will affect an organisation's ability to comply with the provisions set out in the Privacy Act.

**Data Quality**

NPP3 of the Private Sector Amendment sets out expectations for the maintenance of data quality. It requires an organisation to ensure that the personal information it
collects, uses or discloses is accurate, complete and up-to-date. This approach to data quality is quite typical. Much of the existing work on data quality focuses on the intrinsic quality of data in databases and consists of lists of desirable information quality dimensions (Wand and Wang 1996). These lists typically include dimensions such as accuracy, completeness as well as reliability, consistency, timeliness, precision and conciseness (Wang and Strong 1996, Kahn et al. 2002).

As such, these data quality frameworks focus primarily on the content or 'meaning' of particular data fields. That is, they define data quality in terms of the data's semantic properties. However, a wider or more rounded view of data quality can be adopted: a view of data quality that defines quality in terms of the data's 'fitness' for particular purposes or organisational functions (Shanks and Darke 1998). Viewed in this manner, data quality can be seen to involve more than semantic accuracy and completeness. Data has other characteristics such as its structural properties, its useability, and its openness to multiple interpretations in different contexts that also determine its quality or fitness for particular purposes.

Shanks and Darke (1998) have developed an analytic framework based on semiotic theory for the study of data quality in this manner. Their semiotic framework has four discrete levels of analysis: syntactic, semantic, pragmatic and social. Within this framework syntactic data quality refers to the data structures used to store personal information. Syntactic data quality is a measure of the consistency of representation in one or more databases. Semantic data quality focuses on the meaning of data and measures how complete, accurate and up-to-date it is. Pragmatic data quality is concerned with the utility of data for specific tasks and is a measure of the usefulness and useability of data. It will vary with the person involved, the task at hand and the organisational context of use. Finally, social data quality is a measure of consistency of interpretation of data by different social groups within an organisation.

This semiotic framework provides a set of generative concepts and analytic distinctions that are useful for investigating and understanding some of the impediments and problems face by organisation as they move to comply with the provisions of new privacy legislation. It is particular useful because, by defining data quality in terms of fitness for purposes, it focuses our attention on the connection between the qualities of an organisation's databases and the organisation's ability to respond to the regulatory requirements of privacy legislation.

**Research Approach**

This research study was exploratory in nature and involved two main phases: a conceptual phase and an empirical study. The conceptual study phase of the research included a critical review of the Privacy Act and Private Sector Amendment, associated submissions to parliament, press commentary and other relevant literature from both academic and practitioner sources. This material was then synthesised with concepts from Shanks and Darke's (1998) semiotic framework for understanding data quality in order to develop an initial understanding of how poor customer data quality may prevent organizations from fulfilling their obligations to maintain the information privacy of individuals, and to develop an interview protocol for data collection in the empirical phase of the research.
The empirical phase of the study involved in-depth interviews with eight experienced practitioners. Interviewees were identified opportunistically and selection for interview was based on the criteria that they had extensive experience with information privacy and the management of information systems. Five of our interviewees occupied senior, information systems management roles in private sector organizations that handled large amounts of customer data. The other three were consultants specialising in the areas of privacy and/or data management. Empirical data was collected through open-ended and semi-structured interviews and review of documents contributed by interviewees. Interview duration ranged from 60 to 90 minutes and were recorded on audiotape and fully transcribed. Qualitative data analysis techniques (Miles and Huberman 1994) were used to identify key issues associated with data quality faced by organisations as they responded to the provisions of the legislation. From this list of key issues, one issue was selected for discuss in this paper on the basis of its relevance, importance and frequent occurrence. In this paper we discuss the problems created by the fragmentation of personal information about an individual across a number of different databases that are owned and controlled by different function units within an organisation. In particular, we will discuss the difficulties this situation creates for organisations when called upon by customers to complying with the provisions of NPP 6 (access and correction).

Data Fragmentation and the Control of Personal Information

Many large organisations of the type covered by the Private Sector Amendment will have a history of separate business units developing and maintaining independent customer databases. Typically these legacy systems will have been developed autonomously and use a variety of data structures and identifiers to record personal information. In addition, these databases are often 'owned and operated' by separate functional units within the organization. Consequently, the personal information an organisation holds about individuals will be fragmented across a number of databases using a variety of different data structures (Redman 2001). This makes accessing and collating personal information difficult and time-consuming (Redman 1998). Rarely in these cases is there a unified and consolidated view of the personal information an organisation holds about an individual (Shanks 1997).

These kinds of data quality issues that extend across the syntactic level – in the form of incompatible and inconsistent data structures – to the pragmatic level – in the form of data that has low useability and usefulness – make it difficult for an organisation to comply with some of the provisions of the Private Sector Amendment. In particular and most strikingly, it creates problems with the central information privacy tenet associated with giving individuals control over their personal information: allowing individuals to access and correct personal information held about them by an organisation. This principle is codified in NPP 6 of the Private Sector Amendment. NPP 6 – Access and Correction – states that an organisation must give individuals access to their personal information if requested and they must correct that information if it is inaccurate, incomplete or out-of-date. In addition, an organisation may charge for providing access to personal information if those charges are not excessive.

One of our interviewees, the information systems manager for a major metropolitan hospital, said that locating and identifying all the databases within the organisation that contained identifiable personal information was a major problem for his
organisation's ability to comply with the new privacy legislation. While the paper-based patient record recorded all treatment that patients received within the hospital, various units within the hospital also maintained their own, separate records for a variety of purposes associated with research, treatment and service evaluation as well as for the purposes of providing a health service to the patient. In addition, some senior specialists who consulted with patients in the hospital maintained their own, private records and notes on patients independent of the main hospitals patient record system. Senior specialists and the central medical record and patient billing systems aside, this organisation had approximately 30 different function units that collected and used personal information; many of them using more than one information system to so. While a portion of these information systems were modest in scale – spreadsheet applications and small databases – the difficulties this situation created for the organisation in compiling a view of the totality of personal information held about any one individual, are obvious. This degree of fragmentation creates serious pragmatic data quality problems and has severe implications for this organisation's ability to respond in a timely and efficient manner to an individual's request to access their personal information as required by NPP6 (Access and Correction).

Two other interviewees who worked for large retail organisations also reported problems of a similar nature. Although the problems were on a smaller scale, the organisations they worked for were grappling with similar issues associated with multiple and fragmented databases. In both cases, despite having made significant moves towards consolidating customer databases used for a variety of purposes such as tracking purchasing habits, marketing, lay-buy, in-store credit facilities and valued customer schemes, these organisation still had personal information about customers contained in multiple databases owned by different departments within the organisation. One of these organisations, a large retail chain, keep personal information associated with lay-buys in small systems locally maintained in each of its retail outlet as well as maintaining separate databases relating to its credit schemes and marketing activities. The other organisation, a large department store chain, maintained an integrated, centrally controlled customer relationship management system. Yet, it too had some problems with database fragmentation as several departments within the organisation such as human resources, marketing and in-store security insisted on maintaining their own databases that contained significant amounts of personal information. These departments also insisted that other departments within the organisation kept their 'hands-off' these information systems and thus these databases that contained personal information were not subject to any form of unified or centrally coordinated control by the organisation. This fragmentation and the lack of control over personal information it created had particularly serious implications in regard to the sensitive nature of the personal information and opinions about individuals being collected, stored, used and disclosed by the in-store security department. Although no customers of these organisations had requested access and correction of the personal information held by these organisations at the time of interview, our interviewees anticipated that this lack of cohesion in their databases would create significant difficulties with providing customers with access to all the personal information held about them and would impede their organisation's ability to comply with the access and correction provisions of the Privacy Act.
The spread of these kinds of problems across the private sector were confirmed by the three consultants we interviewed based on their experience with a broad range of private sector organisations that operated in a variety of different sectors of the economy.

It is also worth noting that the legislation allows organisations to charge individuals for providing access to their personal information, although 'excessive' charges are prohibited by the legislation. However, the definition of 'excessive' in this context has yet to be established (Sinclair 2002a). Recent press reports indicate that some large organisations intend to use an hourly-rate to calculate these charges on a cost-recovery basis. For example, the four major Australian banks are charging between $25 and $70 an hour for accessing personal information (Sinclair 2002a). Poor data quality created by the fragmentation of personal information across different databases will impact on the time it takes to recover personal information and hence the charges made by an organisation on a cost-recovery basis. Charges made on a cost-recovery basis are unlikely to be deemed 'excessive' unless fragrantly extravagant. This creates the possibility that customers exercising their right of access and correction will end up paying a higher premium for this right as a result of an organisation's poor customer data quality.

**Discussion and Conclusion**
A review of Australian privacy legislation indicates that this growing body of legislation is based on the assumption that organizations have an integrated customer data set and that it is relatively easy for organisations to access, collect and collate all the personal information they hold about an individual. The reality is quite different for many organisations. These organisations do not have an integrated customer data set and cannot readily achieve the unified view necessary for strict and unproblematic compliance with the provisions of this legislation due to problems with data quality.

This problem is particularly pernicious for organisations with multiple points of customer contact. These organisations are often characterised by semi-autonomous functional units that have been in the habit of amassing their own customer databases without reference to a centrally coordinated information management strategy. As a result, the sum total of personal information held about any individual is fragmented across multiple and incompatible databases creating significant data quality problems that severely hinder the formation of a unified and integrated view of the personal information held about any one particular individual. This inability to develop an integrated view compromises an organisation's ability to effectively manage and control its customer data and hence compromises its ability to meet its obligations under the Privacy Act and its recent amendment.

The ability to develop a unified and integrated view of the totality of personal information held about an individual should enables organisations to comply with the provisions of the new privacy legislation in a relatively unproblematic fashion. Establishing and maintaining high levels of customer data quality across all four data quality levels is an important part of developing this kind of view of the personal information held about a particular individual. It is ironic to note that it is precisely these kinds of information systems that are built on good quality, highly integrated databases of personal information that have raised the hackles, suspicions and fears of privacy advocates and political commentators for several decades due to their ability
to enable organisations to practice data-mining and data-matching activities (See for example Clarke 1988, Davies 1997). Yet, it is precisely those organisations with highly integrated and carefully managed customer databases that are in the best position to comply with the provisions of the new legislation.

It is apparent that although the explicitly stated intention of the Private Sector Amendment is to 'give people some control over the way information about them is handled' (OFPC 2001b), poor customer data quality in the form of database fragmentation can undermine the ability of an organization to manage and use, that is control, the personal information it holds. In order to cede or 'give control', one must have control in the first place. Data quality is an important factor in determining the amount of control organisations have over the personal information they hold. Poor data quality erodes an organisation's ability to control the personal information it holds about individuals and this erosion inhibits their ability to comply with the requirements of the new legislation. Establishing and maintaining high levels of customer data quality is therefore a necessary and potentially expensive step that any organisation will need to take in order to be a privacy compliant organisation. This necessity extends beyond maintaining data quality at the semantic level by ensuring that personal information is complete, accurate and up-to-date as required by NPP3 – data quality. Data quality must also be maintained at the syntactic and pragmatic levels if an organisation is to have sufficient control over the personal information it holds to be able to give individuals the ability to access and correct this information.

Finally, it is worth noting that while our focus has been on the Australian legislative context, these findings also have a wider significance. The Privacy Act and its later amendments are based on the OECD's 1980 Guidelines on the Protection of Privacy and the Transborder Flows of Personal Information. Therefore the issues we identify are not limited to the Australian context but can be generalised to all organizations that must comply with privacy laws derived from these OECD principles such as those currently being enacted by the member nations of the European Union.

References
Department of Communications Information Technology and the Arts (DCITA) (2000) Submission from the Department of Communications Information Technology and the Art to the Senate Select Committee on Information Technologies Inquiry into e-Privacy – July 2000.
Federal Privacy Commissioner (FPC) (2000) Submission from the Federal Privacy Commissioner to the House of Representatives Standing Committee on Legal and


**Acknowledgments**

The authors would like to thank Graeme Shanks, Reeva Lederman, and Roselle De Silva for their help in the development of this paper.
Ethical and Privacy Issues in Genetic Databases

Helen Giggins¹ and Ljiljana Brankovic²

¹School of Electrical Engineering and Computer Science
The University of Newcastle, NSW Australia
E-mail: higgins@cs.newcastle.edu.au

²School of Electrical Engineering and Computer Science
The University of Newcastle, NSW Australia
E-mail: lbrankov@cs.newcastle.edu.au

Abstract
With the recent advances in genetic and computer technology, enormous databases containing genetic information have become available for research and other purposes. An example of such databases is the Icelandic Health Database containing health and genetic records about the total population of Iceland. This has raised many privacy and ethical questions, both among health professionals and the general public. Many agree that genetic information bears more ethical and privacy concerns than other health databases. In this paper we review the main privacy and ethical issues connected to genetic information and we pay special attention to disclosure of individual values through statistical analysis.

Keywords: Genetic databases, privacy, data security, computer ethics.

Introduction
With the recent advances in genetic and computer technology, enormous databases containing genetic information have become available for research and other purposes. An example of such databases is the Icelandic Health Database containing health and genetic records about the total population of Iceland. This has raised many privacy and ethical questions, both among health professionals and the general public. Many agree that genetic information bears more ethical and privacy concerns than other health databases. In this paper we review the main privacy and ethical issues connected to genetic information and we pay special attention to disclosure of individual values through statistical analysis.

The organization of the paper is as follows. In the next section we present a genetic primer and comment on the significance of genetic research. In the following section we summarise the ethical and privacy issues arising in this context. Next, we briefly introduce an abstract genetic database model. In the same section we outline the security problem in statistical databases, illustrating it using a genetic database example. The following section looks at various case studies and the final section contains the concluding remarks.

Background
Cells are the fundamental building blocks of every living organism and the human body is made up of millions of cells. The activity of these cells is directed by our complete set of DNA (deoxyribonucleic acid), also known as the genome (NSW Genetics Sheet 1 2001). The majority of our DNA is contained in the cell nucleus in
the form of pairs of chromosomes, with each chromosome containing a string of genes and each gene containing DNA. With the exception of mature red blood cells (which contain no nucleus) every somatic cell in our body contains a complete genome (somatic cells are those which are not egg or sperm). In addition to DNA contained in the nucleus, we also have a small amount of DNA (13 recognizable genes) in tiny compartments in the cell called mitochondria (see Figure 1, courtesy of GeneCRC, http://www.genecrc.org). Mitochondrial DNA can be used in forensic identification even when other genetic material has been degenerated, due to the large number of mitochondria in each cell (Miller 2002).

![Diagram of a cell](image)

**Figure 1: Component parts of the human cell**

Each cell nucleus contains 23 pairs of chromosomes. One chromosome in each pair comes from the mother, and the other from the father (see Figure 2, courtesy of NSW Genetic Education Program, http://www.genetics.com.au). Mitochondrial DNA however, is inherited only from the mother because of the relative size of the egg compared to the sperm cell (Miller 2002).

Each chromosome is a single molecule of DNA. Some sections of a DNA molecule carry genetic information that controls the production of proteins within the cell; these sections are known as genes. Other sections consist of repeated sequences that carry no relevant information for protein synthesis and are referred to as ‘junk’ DNA. To visualize chromosomes, it is helpful to imagine a DNA molecule as a coiled string of beads where each bead on the string is a gene (see Figure 3, courtesy of NSW Genetic Education Program, http://www.genetics.com.au). On average, each chromosome is made up of hundreds of genes. The latest research estimates that chromosome 1 has the most genes (2968), and the Y chromosome has the fewest (231). The total number of genes is estimated to be between 30,000 and 40,000, much lower than previously believed (Human Genome Project 2001).
Each gene consists of a sequence of DNA as shown in Figure 4 (courtesy of NSW Genetic Education Program, http://www.genetics.com.au). DNA contains a string of nucleotide bases, Thymine (T), Adenine (A), Cytosine (C), and Guanine (G). In the human genome there is a total of more than 3 billion bases (Human Genome Project 2001). Within one chromosome there are gene rich areas consisting mainly of C and G bases, and large areas with junk DNA consisting mainly of A and T. These two areas are separated by so-called barrier regions that contain exclusively C and G bases. Although barrier and junk regions do not contain information for synthesis of protein, they are still thought to have an important role in chromosomal activity. Junk DNA makes up at least 50% of the genome, while genes contribute only about 2% (Human Genome Project 2001). The function of only about 50% of genes is known. It is interesting to note that the human genome contains many more repeating sequences than the genome of other more primitive organisms, such as the mustard weed (11%), the worm (7%), and the fly (3%) (Human Genome Project 2001). Despite the fact that
humans do not have many more genes than a fly or a worm, they still have three times as many different proteins due to the numerous ways in which genes combine to create proteins.

![Figure 4: Genes and DNA sequence](image)

The order of bases in the genome is almost exactly (more than 99%) the same in all people (Human Genome Project 2001). The variations in genes that can occur in the genome across the human population are known as ‘alleles’. These discrepancies occur when there is a change in the ordering of the bases, a change of a single base, the inversion of two bases, as well as the insertion, deletion or repetition of a sequence of bases. Some alleles result in no difference to health but, for example, in differences in hair or eye colour. Such alleles are called ‘polymorphisms’. So far researchers have discovered about 1.4 million locations where a single-base polymorphisms can occur. On the other hand, alleles that do have health implications are called ‘mutations’. They can lead to production of abnormal protein, reduced amount of protein or no production at all (NSW Genetics Sheet 2 2001).

The genetic make-up encoded in the genome is called ‘genotype’, while the entirety of genotype and environmental factors is referred to as ‘phenotype’. Some features, such as eye colour, are clearly determined by our genotype alone. Other properties including height are determined by both genetic make-up and environmental influences. The later example can be seen a potential of a person to achieve a height of 185 centimetres. Whether this will occur will depend on diet and other environmental factors. Similarly, a person who has a genetic predisposition to develop Alzheimer’s disease may not develop it at all or the symptoms can be postponed until a very old age. On the other hand, those carrying the gene known to cause Huntington’s disease have close to a 100% chance of presenting symptoms of the disease at some point in their life. There is much debate in the media about how much of our behaviour is determined by genetics and how much by our environment. Clearly there is no single gene determining a personality type, hyperactivity or criminality. However, recent studies show that behavioural properties are more hereditary than due to acquired physical disorders (Plomin et al. 2001).

Currently in the western world genetic research seems to receive both high priority status and substantial funding. The expectations from this line of research include improvement in diagnosis of diseases, detection of genetic predisposition to diseases, developments in gene therapy and the design of drugs tailored to an individual’s genetic make-up. One potential benefit in the area of risk-assessment is the ability to identify individuals who are at a higher risk of developing cancer if exposed to certain hazardous conditions, for instance radiation or toxic waste.
Quite different but also important applications come from anthropology, human migration, evolution and bioarchaeology. For example, the study of mutations in the Y chromosome may be used to trace male ancestry and migration patterns. Applications in criminology typically use DNA matching. These include uncovering potential suspects, vindicating persons wrongly accused of crimes, and identifying victims. Another important application is in matching organ donors and recipients. There are also various applications relating to agriculture and bioprocessing (Human Genome Project 2001).

Ethical and Privacy Issues
Ethical and legal issues in genetic information processing are considered increasingly important and are receiving more and more scientific and public attention as well as funding. For example, the Human Genome Project has allocated up to 5% of the annual budget to ELSI (ethical, legal and social issues) research (ELSI 2002).

One of the basic questions arising in this context is the question of ownership of genetic information. Is the genetic information about an individual owned by the individual, the gathering organization (e.g. hospital) or perhaps the government?

The purpose for which genetic information is to be used is another important concern. Should usage of such information be limited to diagnostic and medical treatment purposes only? Or is it acceptable to use it for other ends, such as criminal investigation, genetically modified food and medical insurance criteria? Could it even be tolerable to use it for immigration, education or employment selection criteria? While the education scenario may sound far fetched, the other scenarios are very realistic concerns as illustrated by the following example. Terri Seargent, a woman from North Carolina, got fired from her job only three weeks after receiving a pay rise and an excellent performance review. Because the firing occurred a very short time after she was diagnosed with a genetic disorder requiring expensive treatment, Terri believes that her employer got hold of the test results and fired her to avoid expenses. In November 2000 the Equal Employment Opportunity Commission supported Terri’s disability allegations against her employer. This gave Terri the right to pursue legal action in order to gain compensation for her wrongful dismissal (Alpha-1 2000).

A National Center for Genome Resources survey from 1998 (Health 2002) shows that 85% of those surveyed believed that employers should not be given access to information about genetic conditions, risks and predispositions. For a comparison, in the same survey 69% of respondents believed that the same information should not be disclosed to health and life insurers. Moreover, 63% said that they would not take genetic tests if employers or insurers would have access to the results. In a more recent survey commissioned by the California Health Care Foundation and Internet Healthcare Coalition (Health 2002) 76% of Internet users in good health are concerned about their health insurer obtaining their health information that they provided to an online Website. The same survey shows that 60% expressed similar concerns towards their employer obtaining such information.

Without careful contemplation and resolution of these controversial issues one can easily imagine a gloomy futuristic society where an individual’s prospects in life can be decided by a simple test at birth. Even in our current societies there are significant concerns relating to stereotyping, stigmatising and discrimination as illustrated by the
discrimination example given above. Furthermore, inequitable accessibility of advanced genetic technologies may deepen the gap between the developed and the developing world and rich and poor individuals within the same society. Additionally, the relationship between genotype and phenotype raises the philosophical question of supremacy of genetic determinism over freewill. However, the situation here is more complex than meets the eye. There are scenarios where the stigmatisation seems to be decreased by the fact that a disorder is of a genetic nature. For example, it is now acceptable for an American ex-president to acknowledge that he has Alzheimer's disease (McGuffin et al. 2001).

It seems to be very hard for laws and legislation to keep pace with the advances in genetic information technology. The Australian Law Reform Commission is currently working to prepare a report for Government on the protection of genetic information (ALRC 2001). There is a prevailing opinion that laws in this delicate area should not be too specific and should not be established too early, before the genetic information is truly understood (Senate Legal 1999).

Yet another important issue is the adequate education of the public, necessary for making informed decisions and giving informed consents. Related to this is the education of health professionals about the accuracy, limitations and reliability of genetic testing (Human Genome Project 2001). When the reliability of the testing or the accuracy of interpretation is low or there is no known cure, should the results be disclosed to the patients? This raises the ethical issues of ‘right to know’ and ‘right not to know’ and the balance between the two (ALRC 2001). There are situations where informing patients about potential genetic risks can be more destructive than useful for the overall health of the patient. This brings us to the wider concern about widespread use of technology not yet well understood and the possible conflict with the basic ethical medical principle: ‘Do not do harm’. This is further illustrated by concerns about the safety of genetically modified food for human consumption (Human Genome Project 2001).

In what follows we shall turn our attention to another important concern, namely the privacy of involved individuals and the confidentiality of their genetic information. Arguably, genetic information is more sensitive than other medical data (ALRC 2001). There are several issues to be considered here. Firstly, genetic information gives the biological essence of each human being – practically, each individual (other than identical twins) is genetically unique. This is not the case with other medical data. Secondly, genetic data of an individual can also have implications for family members and ethnic groups. This raises concerns that genetic information could be used to discriminate against individuals and even whole groups within a community. Finally, genetic data not only discloses information about existing conditions, but also has an inherent predictive nature. It can provide insight into the potential health risks to the individual years into the future. A concern is that possibly imprecise genetic information could be used by insurance companies, employers or public authorities in the decision-making process in relation to the individual.

**Genetic Database Model and Statistical Security Problem**

We shall now present an abstract model of a genetic database that will be used in this section to illustrate subtle privacy threats known as statistical disclosure. The model can be seen as a two-dimensional table where each row represents a patient, and each
column corresponds to a property of the patient. The properties can be categorized as follows.

1. General information including name, address, date of birth, gender, family doctor and other personal details.
2. Medical history including past medical history, hospital admissions, current diagnosis, medication and so on.
3. Pointers to records of parents, siblings, children, and other family members.
4. DNA sequence.
5. Inferences made by analyzing the DNA sequence.

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>DOB</th>
<th>G</th>
<th>FAMILY DOCTOR</th>
<th>LAST HOSPITAL ADMISSION</th>
<th>CURRENT DIAGNOSIS</th>
<th>BLOOD COUNT</th>
<th>M</th>
<th>F</th>
<th>DNA SEQUENCE</th>
<th>GD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Brown</td>
<td>23/05/64</td>
<td>f</td>
<td>1043</td>
<td>12/07/02</td>
<td>ABS234</td>
<td>4.1</td>
<td>3</td>
<td>-</td>
<td>GATCAT...</td>
<td>Y</td>
</tr>
<tr>
<td>2</td>
<td>Brown</td>
<td>6/12/59</td>
<td>m</td>
<td>1023</td>
<td>13/07/02</td>
<td>OCD602</td>
<td>3.4</td>
<td>-</td>
<td>-</td>
<td>GACGAT...</td>
<td>Y</td>
</tr>
<tr>
<td>3</td>
<td>Black</td>
<td>16/03/45</td>
<td>f</td>
<td>1011</td>
<td>13/07/02</td>
<td>MAD102</td>
<td>3.2</td>
<td>-</td>
<td>-</td>
<td>TACGTA...</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>Brown</td>
<td>30/11/84</td>
<td>m</td>
<td>1043</td>
<td>15/07/02</td>
<td>HAV529</td>
<td>4.0</td>
<td>1</td>
<td>2</td>
<td>CGATGA...</td>
<td>N</td>
</tr>
<tr>
<td>5</td>
<td>Jones</td>
<td>28/02/25</td>
<td>m</td>
<td>1011</td>
<td>20/07/02</td>
<td>MAD102</td>
<td>2.9</td>
<td>-</td>
<td>-</td>
<td>TACGCA...</td>
<td>N</td>
</tr>
<tr>
<td>6</td>
<td>Smith</td>
<td>16/07/64</td>
<td>f</td>
<td>1036</td>
<td>21/07/02</td>
<td>IVA908</td>
<td>4.0</td>
<td>-</td>
<td>-</td>
<td>GTCATC...</td>
<td>Y</td>
</tr>
<tr>
<td>7</td>
<td>Black</td>
<td>10/11/72</td>
<td>m</td>
<td>1023</td>
<td>-</td>
<td>WQX733</td>
<td>3.7</td>
<td>-</td>
<td>-</td>
<td>GATTAC...</td>
<td>N</td>
</tr>
</tbody>
</table>

Table 2: Abstract Model of Genetic Database

A simplified genetic database example is shown in Table 1. We note that ‘M’ stand for mother and ‘F’ stands for father. The values of these properties are the ID numbers of the records representing the mother and father of the patient, and if these records are not stored for the mother and/or father, then a ‘-’ is recorded in the database to indicate a missing data.

We shall now concentrate on the so-called statistical security problem, which appears to be largely ignored in the context of genetic databases. This problem arises when a collection of confidential individual data is used for obtaining statistical parameters to facilitate research. While the aggregate values are released to the users, the individual values are deemed to be confidential and should not be disclosed. Thus the system will reject all queries that attempt to access individual values and will only accept the aggregate queries, such as sum, average, minimum, count, etc. Moreover, it should be impossible for users to infer these individual values from any sequence of aggregate values. When a user is able to determine the individual values this is called a database compromise or statistical disclosure.

Furthermore, a weaker inference about the likelihood of a particular value being in a given range of values may as well be considered a compromise. Additionally, the fact that the individual data does not have a particular value may also constitute a compromise. In the absence of any protection mechanism it is fairly easy to compromise the database. To illustrate this we consider a sample genetic database given in Table 1. Consider the following example.

| Q1: How many male patients born before 1956 are there? | A1: 1 |

Page 45
This query uniquely identifies patient Jones, as the only male patient born before 1956. With this knowledge it is straightforward to disclose all of the confidential properties of this patient as shown below.

<table>
<thead>
<tr>
<th>Q2:</th>
<th>What is the total blood count of all male patients born before 1956?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2:</td>
<td>2.9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q3:</th>
<th>How many male patients born before 1956 with a diagnosis of ‘OCD602’?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3:</td>
<td>0</td>
</tr>
</tbody>
</table>

Here we learned that patient Jones has a blood count of 2.9 and he does not have a disease with the code ‘OCD602’.

Clearly the first step in providing security is to disable all statistical queries that are based on a single record. Even with this precaution it is often not difficult to deduce confidential values in a few steps as shown in the next example.

<table>
<thead>
<tr>
<th>Q1:</th>
<th>What is the total blood count of all male patients?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1:</td>
<td>14.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q2:</th>
<th>What is the total blood count of all male patients born after 1955?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2:</td>
<td>11.1</td>
</tr>
</tbody>
</table>

By subtracting the answer to the second query from the answer to the first query we obtain the blood count of the patient Jones with ID =5.

The statistical security problem is an intricate one and is typically dealt with in one of the following two ways. One way is to restrict queries that users are allowed to pose. Another way is to add noise to the data, so that even if an individual value is disclosed the intruder still has a degree of uncertainty about the exact value of the data. In either case it is important to find the right balance between the security and the precision and usability of the database. An excellent survey on existing protection methods is given in Adam and Wortmann (1989). The statistical security problem is yet to be solved in the context of genetic databases, and most literature in this area simply ignores the issue.

**Case Studies**

There are numerous examples of genetic research databases used around the world. Most of them are smaller scale databases created by individual organisations in order to support their own research. Typically, such databases contain genetic samples and tissues as well as genealogical and health information. This information is usually obtained from either consenting patients with a particular disease, or volunteers. An Australian example of such a database is the Peter MacCallum Cancer Institute’s tissue bank, used for cancer molecular genetic studies (Peter MacCallum 2002). Apart from the cancerous tissues, the database contains blood samples and a rich clinical history. The samples remain identifiable to allow continuous collection of clinical
history, while the de-identified version of the database is available to registered researchers. Another Australian example is the Menzies Research Institute database. This database contains genealogical data and genetic samples, as well as health information about donors, who are all research volunteers (Menzies 2002).

Examples of large-scale genetic databases include Biobank UK, Estonian Genome Project and the Icelandic Health Sector Database (ALRC 2002). Biobank UK is a publicly funded project and all the information contained in it is freely available to researchers. It will contain genetic samples, lifestyle details and health information of up to 500,000 British volunteers (Wellcome Trust 2002). Another example of a large-scale database is the Estonian Genome Project financed and controlled by the public-private partnership between the Estonian Genome Project Foundation (EGV) and Egene, the exclusive commercial licensee of the database (Estonian 2002). The database will contain the genetic information from three quarters of the country’s population (1,000,000).

In what follows we shall concentrate on the third example, namely Icelandic Health Sector Database. In December of 1998 the Icelandic Government passed a bill to form the ‘Act on a Health Sector Database’. The objective of the act was to increase knowledge and hence improve health services through the creation of a centralized database of non-personally identifiable medical data (Iceland Ministry of Health 1998). To be called the Icelandic Health Database, the project will consist of three separate yet connected databases, the Health Database, the Genotype Database and the Genealogical Database (IDPA 2001). The Government has issued a license to a private company (an American registered company, deCODE Genetics Inc., based in Reykjavik, Iceland) to create and operate the database. Importantly, this is the first time the Icelandic Government will have access to centralized medical records.

The intention of the Icelandic Government is to maintain the three databases as statistical databases working in isolation and combination. It should not be possible for authorized users to obtain information about any identifiable individual when performing statistical queries on the Icelandic Health Database (IDPA 2001). According to deCODE there will be various security measures employed to ensure system security. The architecture consists of separate modules that perform the tasks of data collection and validation, secure data transfer, automatic data anonymisation, auditing, and modules for handling data storage and analysis (deCODE).

The way in which the information will be collected for each of the three individual databases differs. The Health Database will gather information from the Icelandic healthcare system, using presumed consent. The information collected for the Genotype Database will however require the informed consent of donors before it is stored (deCODE). Since Iceland’s genealogical history is presumed to be in the public domain there is seen to be no need to obtain consent for the use of this data in the Genealogical Database component of the project (deCODE).

There has been much public concern and controversy surrounding the implementation of the Icelandic Health Sector Database (Mannvernd). One of the most controversial aspects of the Health Database component is the use of presumed consent in its creation. Patients are presumed to consent to the use of their medical history for an unspecified range of research purposes. They may at any point opt out of having
further information about them stored but this does not extend to having existing data about them removed from the database. In medical ethics informed consent is usually seen as the preferred option as it not only protects the privacy of individual research subjects, but also protects their autonomy (Greely 2000). With informed consent subjects they can make their own evaluation of the privacy risks and make their own decisions about their involvement.

The Data Protection Authority has set out guidelines for deCODE in the creation of statistical inference countermeasures. These measures include query set size control restrictions with the minimum query set size being set to ten (IDPA 2001). The security function will also employ noise addition techniques, however, the actual technique and parameters have not been specified (IDPA 2001). The original specifications did not include any statistical protection whatsoever, and the above measures were only added after harsh criticism by Ross Anderson (1998), an expert in computer security.

Another point of criticism offered by Anderson (1998) is the way in which personal information is de-identified in the system. The only specified measure for de-identification of medical data is the removal of obvious identifiers such as name, with encrypted social security numbers used as personal identifiers for records (IDPA 2001). However, it is important to note that these measures are not sufficient to provide complete anonymity as any combination of attributes that uniquely identifies an individual can be used to infer confidential individual values (Anderson 1998). This clearly indicates that more effort is required to provide an adequate level of security in the Icelandic Health Sector Database.

The Icelandic experience provides a valuable lesson when deciding on the future direction of genetic database research in Australia. Currently the Australian Law Reform Commission (ALRC) and the Australian Health Ethics Committee (AHEC) are conducting an inquiry with respect to the protection of human genetic samples and information. The joint inquiry was announced in August 2000 and the final report is due in March 2003, where the deadline has been extended due to public demand (ALRC 2001). A lengthy public consultation has already taken place with submissions being accepted from any member of the public, and the ALRC and AHEC have recently published a joint Discussion Paper (ALRC 2002).

**Conclusion**

In this paper we outlined a number of ethical and privacy issues that have been raised by the emerging field of genetic databases. Some of these issues are unique to genetic information and do not apply to other sensitive medical databases, and as such require special consideration. It is very difficult for the legislation to keep pace with the fast evolving nature of this area. Of particular importance is the problem of statistical database security, which has not yet received enough attention in literature and practice. Even in genetic database systems of a very large scope, such as the Icelandic Health Database, this problem has not yet been successfully solved. Moreover, there seems to be a lack of awareness about it by the general public and security experts alike. However, there is substantial experience related to census and other traditional statistical database applications, which should be built upon to satisfy the specific requirements of genetic databases.
References


Ethical Issues for Professional Web and Software Designers: Are there 2 classes of users?

Brian Hardy¹, and Oliver K. Burmeister²

¹Manager Information Services Development
Vision Australia Foundation, Australia
E-mail: brian.hardy@visionaustralia.org.au

²Swinburne Computer-Human Interaction Laboratory
School of Information Technology
Swinburne University of Technology, Australia
E-mail: oburmeister@it.swin.edu.au

Abstract

Professionalism in every field requires consideration of one’s clients or customers. When a small but significant minority of customers are consistently ignored, by IT developers, then their conduct cannot be considered professional. Such is the case with considerations of access alternatives for users of IT not able to make efficient use of conventional access methodologies. This paper raises awareness of the issues and suggests a framework for professional developers to guide them through appropriate behaviours to this important segment of their customer base.

Keywords: Professionalism, accessibility, web design, software design.

Introduction

This paper applies what has been written elsewhere on professional conduct (Spinello, 1997; Gotterbarn, 2000; Burmeister, 2001) to a specialised area of IT often neglected. That is, professional practice by web and software developers in relation to access considerations.

Web designers have numerous sources for best practice when it comes to navigational structures, content separation from presentation, use of database supplied content, the application of World Wide Web Consortium (W3C) standards in the design of server side and client side applications, and more. Non-internet software developers likewise have well established guidelines for development paradigms.

However, much of the development effort is aimed at the majority of users. This is evident in fields such as usability testing where the emphasis is frequently on taking just a small selection of users to identify 70-80% of usability problems quickly, before the next iteration of the design is created and then further tested.

This paper suggests this leaves a second class of user largely unconsidered. Some users have needs for alternate means of accessing either the web or other software products. Reasons for this vary. It may be that the user is based in rural Australia
where connection speeds to the internet are slow and disruptions to connections frequent. 30% of people in rural Australia surf the net with images turned off to help mitigate the effect of slow download speed (Groves, 2000); this makes many sites inaccessible to them. It may be that the user is ageing and has age related functional disabilities, such as arthritic problems that limit use of common navigational devices such as a mouse. It may be that the person has a disability, such as vision impairment, which necessitates use of screen-reading technology, that renders printed information in audio form. Combinations of access problems are also possible.

People can also suffer temporary situations of impairment hindering use of technology for a time. For example a simple accident that injures a hand, arm or shoulder may mean that a key employee cannot use a mouse. If the corporate internal systems cannot be used easily from the keyboard alone, the employee will not be able to function effectively for several weeks.

Why should I care?

This is a valid question for the developer. Others to consider might be:

• Do I have an obligation to try to design something that is accessible to all the potential users or just to some users? If only some users, which users? And why these users?
• What are the implications for my client if I design something that is inaccessible to some users? Could there be implications for me or my employer?
• What are the implications for potential users of the site or software I design if they cannot access it?
• Is the law relevant to this issue?
• Are there ethical issues for me as a professional?
• Is this an issue that I should care about?

Professional responsibilities

In part the answers to the above questions reduce to an exercising of one’s professional responsibilities toward one’s clients and towards the eventual users of the technological products being developed. Amongst the four features Spinello (1997) lists that qualify people as professional in any field are an expectation of contribution to society through services provided and an assumption of autonomous judgment in work carried out based on expertise. Sentiments like these are echoed in various parts of the Australian’s IT professional code of ethics as well. Within the Australian Computer Society’s (ACS) code there are numerous injunctions for conduct toward clients, eventual users and the general public that pick up Spinello’s views for IT professionals. For instance, the requirement to continually upgrade one’s knowledge and skills as part of one’s ‘Professional Development’. More generally IT professionals need to remember that adhering to the code and being seen to do so is
part of the public responsibility the IT profession has. This is seen in the following statement by the Australian Council of Professions (ACP) as professionals:

“It is inherent in the definition of a profession that a code of ethics govern the activities of each profession. Such codes require behaviour and practice beyond the personal moral obligations of an individual. They define and demand high standards of behaviour in respect to the services provided to the public and in dealing with professional colleagues. Further, these codes are enforced by the profession and are acknowledged and accepted by the community.” (ACS, 2000)

**Socio-economic considerations**

Access to the web and other software by the aged and people with disabilities needs to take into account that this requires use of low-cost technologies, readily available to people in the lower socio-economic bands of society. The Human Rights and Equal Opportunity Commission (HREOC, 1999) say that the people with disabilities are in the lowest socio-economic levels of society. Similarly 48% of retirees are among the poorest 30% of Australians (ASFA, 2001). Most older Australians are on a low income with 75% of the eligible population receiving government pensions as their principal source of income (ABS, 2001).

One of the authors was told by a developer that if users with access problems simply upgraded to the latest technology platform for his particular domain in web design, then the problems being voiced would no longer exist. Unfortunately most of his disabled users were not even close to his income bracket and such an upgrade would have been well beyond their means. Yet he did not see the need to make the site he was developing accessible to older technologies. This type of attitude is in the experience of the authors all too prevalent in the developer community. This is particularly true of web development, where as Nielsen (2002, p 2) writes, development for senior citizens is often carried out by young people who too readily “assume that all users have perfect vision and motor control, and know everything about the Web. These assumptions rarely hold, even when the users are not seniors.”

**Legislation**

Government sites by the end of 2001 were mandated to conform to at least single “A” level of the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) standards, seen as best practice in Australia (Sampson-Wild and Burmeister, 2001). Yet the recent call for tenders to audit compliance of Government sites, which closed 20th June this year (Innes, 2002), is likely to find very few government sites complying to these standards as yet.

Some compliance has been ‘encouraged’ through the successful litigation brought against the Sydney Organising Committee for the Olympic Games (SOCOG), by a visually impaired user of their web site (Sampson-Wild and Burmeister, 2001). Further litigation may soon be forthcoming. A US based disability advocacy group is now openly advising disability groups in Australia to forward to them web sites of Australian businesses who have actual or potential US customers. They are able to
initiate litigation for non-compliance under the US law, where no equivalent litigation is likely to succeed within Australia.

**A Proposed Ethical Framework for access considerations**

To address these concerns an ethical framework relating to access considerations is needed. This should be consistent with the broader IT Professional Code of Ethics, but should specifically address a professional’s responsibility in relation to accessibility issues.

**Advising your client**

Web and software professionals have an obligation to advise their client about the appropriate accessibility guidelines and about the implications of not addressing accessibility issues. This advice should be provided at the start of a project.

**Costing accessible design**

Web and software professionals have an obligation to advise their client of the marginal costs of developing designs that are accessible. These costs should assume that the designer/developer was knowledgeable and experienced in accessible design. Unless the client is requesting work that is at the boundary of current accessible design techniques, the client should not have to pay extra for the designer/developer to obtain the skills and knowledge needed to deliver a high professional standard of accessible design.

**Professional skills in accessible design**

Designers and developers (and their employers) have an obligation to realistically assess their own skills in accessible design and take the necessary action to bring those skills up to a high professional standard and/or engage people with specialist skills in accessible design to assist with each project. This should be seen as a core skill for all professionals so should be a priority in professional development.

**Presenting design choices**

Designers and developers should always present clients with a design option that maximises accessibility, consistent with the client brief. The client should be advised about the accessibility implications of each design choice offered. They should also be advised of the costs of retrofitting, should the client later decide to make the site accessible. Designers and developers should use their best endeavours to assist the client to have the most accessible software or web site.

**Reporting on accessibility**

Designers and developers should report honestly and completely on any accessibility issues not resolved with the final product. This provides the client with an opportunity
to put in place other measures to mitigate the impact of the inaccessible elements of the site or software.

**Conclusion**

A civil engineer would not design a bridge that 20% of vehicles could not cross. Yet it is common for software and websites to be inaccessible for some people or difficult to use for a many people. There is a need to raise awareness in the developer community. This is being done internationally by the W3C WAI and nationally through WAI sponsored events such as the annual OZeWAI workshops, and other initiatives such as those of Sampson-Wild and Burmeister (2002) to raise awareness in the web development community about user agents and assistive technologies that can be used to better include people with disabilities in online communities.

Yet even W3C members give mixed messages, by not practicing what they preach consistently. This is shown by Karppinen (2002): “As it happens, out of the 506 W3C members, only eighteen have web sites that validate with the W3C Validator as either html or xhtml. 141 members proudly display sites with definite markup errors; a whopping 342 sites couldn't be tested at all because of lacking DTD definitions. Sad.”

A professional approach to web and other software design is to make a business case for the work required. The developer has to make an informed judgment about the design proposed. Though the threat of litigation is a reality in some cases, the motivation for accessibility considerations as part of the overall design considerations should be driven not by fear of this but rather by one’s professional pride. Attention to all aspects of the design are an integral part of one’s professional practice. Doing so ensures that the current class distinctions between those with access and those without, will soon be a thing of the past.

**References**

Australian Bureau of Statistics (2001) Population by Age and Sex, Australian States and Territories, Cat No 3201.0, Canberra, December 2001


Groves, J. (2000), Web Sites for Rural Australia: Designing for Accessibility, Rural Industries Research and Development Corporation, RIRDC Publication No. 00/13


Internet Banking: Security, Ethics and Trust

Damien Hutchinson and Matthew Warren
School of Information Technology, Deakin University, Geelong,
Victoria, Australia
E-mail Contact: drh@deakin.edu.au

Abstract
Trust is the foundation upon which E-commerce (EC) is built. The Internet was initially designed for information and resource sharing. The design considerations did not include means for performing electronic transactions. The initiation of transforming business operations on-line in both areas of business to business (B2B) and business to consumer (B2C) commerce translates to the requirement for the secure means of conducting electronic transactions which in the majority of cases will involve the use of Internet banking. Numerous incidences of computer crime have shown the vulnerability of transactions to security threats enforcing the need for the construction of mechanisms to build sustaining trust relationships between business partners and to maintain customer satisfaction between parties conducting EC transactions. This paper deliberates between the issues of EC and business, security of transactions via this medium and the paper offers a conceptual trust model upon which these transactions can be constructed.

Keywords: Internet Banking, Security, Trust and Ethics.

Introduction
Trust formed the base upon which traditional commerce was built. E-commerce (EC) does not change this rather it challenges many of the trust assumptions and processes that paper commerce now takes for granted (Keen et al., 2000). The Internet was initially designed for information and resource sharing. The design considerations did not include means for performing electronic transactions. The initiation of transforming business operations on-line in both areas of business to business (B2B) and business to consumer (B2C) EC translates to the requirement for the secure means of conducting electronic transactions, which in the majority of cases will involve the use of Internet banking. Numerous incidences of computer crime have shown the vulnerability of EC transactions to security threats and like the introduction of new information technologies (Mason, 1986; Clarke, 1988) the underlying technologies aimed at securing this open environment are subject to security concerns.

The future outlook of EC will be dependant on controlling information security threats, enhancing consumer security perceptions (Friedman et al., 2000; Schneiderman, 2000) and building trust (Hoffman et al., 1999; Keen, 2000). Given the enormous investments to increase security and trust in EC it is essential that mechanisms be designed for trusting this medium. The authors are extensively involved in security research in regards to Internet banking and are currently working with Australian businesses and banks to develop security models for Internet Banking Security. This paper represents an extension of that security research, in developing a
trust model to complement the security models that they have developed.

**A Definition of Trust**

The term trust is defined as the reliance on integrity, justice etc, of a person, or on some quality or attribute of a thing, confidence (Macquarie, 1997). Other definitions include “trust is a term with many meanings” (Williamson, 1993), “trust is itself a term for a clustering of perceptions” (White, 1992), etc, there is not one single definition for the term ‘Trust’. One of the problems in defining what trust is, in a generic manner, is that researchers continue to express concern regarding their collective lack of consensus about trust’s meaning (McKnight and Chervany, 1996).

To overcome this, researchers at the University of Minnesota proposed a generic trust model, it defined trust as consisting of the following components (McKnight and Chervany, 1996):

- Trusting Behavior;
- Trusting Intention;
- Situational Decision to Trust;
- Dispositional Trust;
- Trusting Beliefs;
- System Trust;
- Belief Formation Trust.

The development of EC meant that the previous research into trust had to be expanded to take into account new issues, the role of trust within a global market that operates twenty four hours a day. This meant that new trust models had to be developed in order to deal with the complex issues involved in EC.

One of the key aspects in regards to EC is that trust is involved in on-line transactions, users are unsure whether to trust EC because of the anonymous nature of it and the perception of risk that they relate to it (Leitch and Warren, 2000). This involves ethical considerations including issues of anonymous and pseudonymous transactions, privacy implications of digital signatures as well as customer profiling. The need for trust is further emphasised by the view that ‘computer hacking’ is understood by those who engage in this behaviour not as criminal or unethical but as exciting, instructive or intellectually challenging (Huff and Finholt 1994). Low figures of reported incidence by organisations who have fallen victim to computer crime can be attributed to the unwillingness of revealing the actual nature of the computer crime for fear of losing public trust (CSI 2002). Given the overwhelming number of thieves are trusted by honest insiders it is vital that the ethical and social aspects associated with more traditional crimes against persons or property be applied to Internet banking transactions so that those who associate various forms of computer abuse as ethically inappropriate will be more likely to refrain from such behaviour (Huff and Finholt 1994). By outlining a standard which defines the manipulation of Internet banking transactions as unethical would be a step towards instilling trust in such transactions. This is inline with the guidelines of the ACM Code of Ethics that specifies an obligation to protect data about individuals from unauthorised access or accidental disclosure to inappropriate individuals (imperative 1.7) as well as organisational leaders having the obligations to verify that systems are designed and implemented to protect personal privacy (imperative 1.8) (ACM 1992). By specifying a conceptual
model for security and trust within Internet banking transactions it is anticipated that the important relationship of ethical considerations for this environment will emanate as a means of appropriately handling Internet banking transactions.

Other research has shown that many of the risks related to EC relate to the transaction involved. The issues of transactions and trust can be explained by looking at the information available to the parties during an on-line transaction. The three information situations are (Tan and Theon, 2000):

- the situation of perfect information in which all parties know everything that is relevant for a transaction;
- the situation of complete ignorance where none of the parties has information relevant for (a part of) a transaction;
- the intermediary situation of information asymmetry in which one party has information that the other party does not have.

This concept that EC trust was concerned with transactions was formally developed into a generic trust model for EC (as shown by figure 1). The main aspect of the model is that transactional trust is the key area of EC and trust (Tan and Theon, 2000).

![Figure 1. Generic Trust Model for EC (Tan and Theon, 2000)](image)

This generic EC trust model does not help when computer security and trust is considered. Most of the work concerning trust in computer science have been concentrated in the area of security. This is mainly in the form of formal logics to analyze cryptographic protocols for design flaws and correctness (Abdul-Rahman and Hailes, 2000).

As mentioned previously, the authors research focus has predominately been within the research area of computer security. In the area of computer security a trusted system is often intended to be a system that is evaluated against certain well defined
criteria like for instance the Trusted Computer System Evaluation Criteria (TCSEC) or Common Criteria (Tjernell, 2000). From this trust becomes a property of a system that can be formally modelled, specified and verified (Denning, 1996). In this setting consumer trust in EC transactions is defined as the subjective probability with which consumers believe that a particular transaction will not occur in a manner consistent with their confident expectations. This maps to the definition of trust where it captures the traditional view of trust in a specific online entity (merchant, bank) and includes trust in the reliability and integrity of the communications medium (Chellappa and Pavlou, 2001).

Another important issue is that perceived information security is the subjective probability with which consumers believe that their personal information will not be viewed, stored, or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations. For instance, a 128-bit encryption objectively gives the odds of a hacker decrypting a message as one in $2^{128}$ (Chellappa. and Pavlou, 2002). This does not directly affect the user, but their perception of risk and willingness to use secure services does, therefore the authors decided to develop a security trust model to deal with transactions and related security mechanisms.

**Security and Trust in Internet Banking Transactions**

When dealing with Internet banking transactions it is imperative that an agreed upon level of trust is maintained throughout the transaction, most probably through mechanisms that guarantee the protection of consumer information in terms of data integrity, confidentiality and privacy which are central to securing the internet banking transaction over the communication network. The failure in any one of these mechanisms at any point within the transaction will result in the security of the transaction being compromised. There have been numerous breaches that have demonstrated such compromise. The motives behind such attacks can be anyone or a combination of the following (Keen et al., 2000):

- Theft or destruction or corruption of valuable data;
- Destruction of network integrity;
- Denial of services;
- Tarnishing of reputation.

Trust has always been a significant factor in influencing customer behaviour towards merchants (Schurr and Ozanne, 1985) and has been demonstrated to be of major importance in uncertain environments like those pertinent to Internet based EC (Fung and Lee, 1999). Security attacks sustained by merchants and Internet retailers from intrusions by hackers not only result in revenue loss and high costs for fixing, maintaining and protecting their systems, but they also project adverse perceptions of transactional security for consumers (Chellappa and Pavlou, 2001). Similarly consumers do not trust Internet marketers sufficiently to engage in "relationship exchanges" involving money and personal information (Hoffman et al. 1999). The trust model for the consumer in traditional commerce is based upon store reputation, brand names and the face-to-face communication that is present in physical interactions (Chellappa and Pavlou, 2001).
In a framework for EC security (Labuschagne, 2000) and a framework of authentication for Internet banking (Hutchinson and Warren, 2001) the elements of authorisation, authentication, integrity, confidentiality and non-repudiation are listed as essential components of securing the EC transaction. The majority of EC transactions are carried out through Web browsers that are connected to merchant sites that in turn connect to some form of financial institution. Like any sound information system the transition when conducting such a transaction should be seamless and transparent for the user but feedback needs to be displayed in order to generate a feeling of control. Some assurance of trust is displayed in browsers and Web sites in the form of symbols for consumers conducting transactions that conform somewhat to these frameworks. Typically an unbroken padlock is used to indicate a secure session facilitating integrity and confidentiality via encryption, statements about data protection and firewalls representing protection, familiar and verifiable domain names for verification and digital certificates ensuring authentication from trusted third parties (Chellappa and Pavlou, 2001).

From a consumer perspective the issue of trust can be ensued by having the following trust elements embedded within the trust model (Chellappa and Pavlou, 2001):

- Protection: This can be defined as the process through which customers are satisfied that their personal information is sufficiently preserved by the entity collecting the information;
- Verification: The inherent lack of implicit identity verification that can be linked with an electronic transaction means that a spurious Web site could easily be created. In relation to Internet banks customers may make the mistake in the domain name, 'www.Citibank.net' instead of 'www.Citibank.com' or may misspell Citibank with a "y" instead of an "i" as in Citybank (Chellappa, 2001);
- Authentication: This is defined as the process through which an Internet merchant can be established via a trusted third party that guarantees that the merchant is indeed who they say they are;
- Non-repudiation: Mechanisms to ensure that client (customer) can be certain it is communicating with the genuine server (Bank) or vice versa, such that neither of the communicating parties can later falsely deny that the transaction took place.

**A Conceptual Trust Model for Internet Banking**

There have been many approaches and standards released comprising details of managing security by implementing appropriate security technologies. Polices have been written to advise who should have access to what information and procedures of how this information should be obtained. All these approaches work well in theory as a methodology in tackling isolated cases. In practice security needs to be dynamic, adapting to changes that occur in the systems underlying changes to the networks the systems are running on. These approaches to security seem to ignore the premise that security is not a technology rather a process that can only be effectively implemented by properly setting sound boundaries and applying the tools and methods available in a team orientated environment. The transacting parties can repeatedly apply the process aiming to improve and keep the security of their systems up to date. Once the process ceases, security is compromised as new threats and techniques emerge (Wadlow, 2000). Following these principles, this section presents a conceptual trust
model incorporating the available security technologies for consumer Internet banking using a process-based approach.

Many payment systems have been proposed for on-line electronic transactions (O'Mahony et al., 2001). In the majority of these systems the bank plays the role of the payment facilitator. The following outlines the architecture of an EC transaction where the customer is purchasing a product or service from a merchant Web Site with the bank providing the actual exchange of payment. The means of payment is via a credit card. There are essentially two separate transaction models that impact the inherent security mechanisms and origin of trust from the customer point of view. The first model displayed in figure 2 is based on having all the credit card information stored at the bank site and only used when on-line processing takes place.

![Payment Systems Architecture - Credit card information stored at bank site](image)

The second model is where the merchant keeps record of credit card numbers and interaction with the bank occurs in a batch like fashion. This introduces security implications like the need for extensive perimeter and database security, that apart from summing to an option that is both costly and effort intensive specifically for business implementation and maintenance, makes the perception of trust for the customer far more volatile. For the reasons of security and speed of setup, the modelling of security into this transaction process concentrates on the first model, which is based on a hosted payment environment where the credit card information is entered on a payment page that is generated from the bank. The outline of the transaction is displayed in figure 3.
The transaction begins with the customer browsing and selecting a product or service from the merchant Web Site that is handled by the merchant pre-payment page. Once the customer has submitted their information for payment the trust model relies on the security implemented between the interactions of the merchant payment page and the bank payment page. The merchant pre-payment page by passing customer information to the bank payment page initiates these relations. At this stage it is at the merchant’s discretion whether the credit card page is presented for the entry of customer information as a separate window or contained within the merchants environment. The customer information populates predefined fields like the card name and the customer then is able to enter their credit card details. The renowned security implementation of the Secure Socket Layer (SSL) whereby the customer is in a full 128 bit-encrypted environment, hosted from the bank production system, becomes the sole safeguard for securing the session. Once the customer details are entered and are submitted, indicating the desire to proceed with the order, the transaction data is passed to the bank for processing. To complete the transaction process the bank responds by generating a payment receipt for both approval or declined transactions, closes the processing page referring to the page where the customer enters their details and sends a SUCCEED (Approved Transaction) or FAIL (Declined Transaction) URL back to the merchant to enable them to create their own page or pass on these parameters to their own backend systems. From this the only trust that the consumer can believe is based on visual symbols such as the brand of the bank and the closed padlock indicating the security within their session supplied by SSL.

The following is a scenario that illustrates the limited protection that such technologies as SSL can provide (O’Mahony et al., 2001). Suppose an adversary has the objective of obtaining identification numbers (IDs) and passwords from an on-line banking service. This perpetrator has the knowledge that the transmissions between the browser (client) and server (bank) are protected by encryption (SSL). To bypass
this technological solution he or she places pamphlets at the banks ATMs encouraging customers to try a new and improved version of the service at www.bank_new_service_site.com (in this example a false domain name). These customers are unaware that the adversary has basically replicated the front page and sign on process of the actual online banking service. When the customer attempts to sign on, the adversary simply captures the IDs and passwords and indicates that the service is not currently available and reroutes the user to the original site. Despite the ability to tamper with customer accounts, the real damage is to the reputations of the customer (which may be the merchant) and bank, which epitomizes a more severe effect than a simple one-time loss of funds. Such scenarios represent the requirement for effective implementation of security and trust in this environment.

A Process Based Model for Trust within Internet Banking

The illustration of the previous scenario was not to place demise on the effectiveness of current available security technologies but rather to exemplify that in order to create sustained trust the approach to security needs to be one that is based on breaking down and identifying individual components of an electronic transaction and mapping what technologies are available to provide assurance where possible. Significantly although there are means of securing a session between the parties in an electronic transaction (in the case described the customer, the merchant and the bank via SSL) the bigger picture including network infrastructure whereby millions of parties are interconnected means that breaches as previously demonstrated cannot be dismissed as adversaries can emanate from various internal and external locations. The transaction overview presented in the previous section can be separated into a series of processes that can be defined as separate entities, each requiring a formal security specification and implementation. Based on the transaction identified these processes can be defined as follows:

- The storage (temporary) of the customer information in the merchant pre payment page;
- Merchant passing customer information to the bank payment page;
- Generation of payment receipt; and
- Transmission of approved or declined transaction.

In relation to the use of a credit card for the means of payment in a secure and trusted manner, the following factors must also be considered within this environment (O'Mahony et al., 2001):

- Card validation: ensuring the current card is valid;
- Cardholder Authentication: confirming the cardholder is the genuine cardholder;
- Merchant Authentication: certifying that the merchant is a bona fide member of a payment scheme like Visa or MasterCard; and
- Privacy: endorsing that the details given during the transaction are handled securely and not available to unauthorised parties.

Figure 4 demonstrates a conceptual model of trust in relation to securing the transaction between the consumer, merchant and Internet bank for the purpose of ensuing the required level of confidence for the widespread uptake of EC transactions.
Figure 4. Conceptual trust Model

This process can be further broken down to show the security implementation at each one of the layers that characterise the EC information transformation for a particular transaction. Figure 5 provides a representation in a hierarchical type structure (Keen et al., 2000) incorporating the integral element of trust.

Figure 5. Security techniques for EC transaction transmission layers

The level of trust that is established in the conceptual model must be maintained from end-to-end in any given transaction. Specifically the trust model employed must be established at the beginning and checks made during the duration of the transaction such that no modification or tampering takes place before the conclusion of the transaction. The technical mechanisms outlined like SSL and other encryption-based methods can act as interim solutions to maintaining this trust. Such technologies though cannot protect against password sniffing or cracking software, spoofing attacks or denial of service attacks. The presentation of numerous incidents in the past and even more so in recent times has undermined the forte of these technologies especially in relation to Internet banking. Thus there becomes a requirement for some form of authentication procedure. In a networked environment this must be implemented between the client and the server to ensure against non-repudiation, such that the client can be certain it is communicating with the genuine server or vice versa. This could be implemented in the form of a digital signature. Regardless of the technologies that may be used to prevent some of the attacks, the outcome of a successful system infringement remains unchanged. Besides compromising data relating to orders and possible fraudulent activities resulting from copying product information, the most damaging effect would be the adverse publicity (Hutchinson and Warren, 2000) and mending customer confidence especially when businesses are already striving for market share and expansion of their customer base in a very competitive unyielding business world.

Conclusion

EC is bridging the gap for both personal and business use, enabling more convenient transactions (via the Internet) but the associated security threats are real and potentially damaging. Threats pertaining to EC have direct impact on Internet banking security. The vital roles that consumers, merchants and financial institutions
play in maintaining the trust bond relies on securing Web clients, the data transaction, the Web server and the underlying network protocol on which the Internet is based. This paper has highlighted the importance of the relationship between security and trust in EC transactions demonstrating that this relationship can be derived from combining the fundamental concepts of EC, made up of the various business issues and the technologies that facilitate the services and applications that define the existence of EC. The case for a new method of formulating such trust was presented in the outline of a conceptual model that employed the idea of processed-based security. Specifically this approach serves the purpose of breaking down the components of an EC transaction to the point where a mapping of security implementations can be viewed as providing trust at the different levels of the transaction process. Critically although the technologies available do provide means via which particular parts of EC transactions can be secured, in the end the ubiquitous uptake of B2B and B2C EC for conducting financial transactions on a large scale will only result from the implementation of an effective model that has both businesses and consumers proclaiming “we can trust this system”.

References


Privacy Protection – Can we afford to Wait?

G. King-Siem\textsuperscript{1}, and I. Morrison\textsuperscript{2}

\textsuperscript{1}School of Information Systems  
The University of Melbourne, Australia,  
E-mail: gmksiem@pgrad.unimelb.edu.au;

\textsuperscript{2}School of Information Systems  
The University of Melbourne, Australia,  
E-mail: iain@staff.dis.unimelb.edu.au;

Abstract  
Personal information is big business, worth over one hundred billion alone between the United States (U.S.) and the European Union (E.U.). Although a significant part of the information economy, trade in personal information is being unduly hindered by differing standards of privacy protection around the world.

Currently, privacy protection varies markedly between different jurisdictions. Some jurisdictions offer high levels of protection whilst others offer little to no protection. Although Australia has recently upgraded its privacy protection to include the private sector, it still falls short of the European standard. Whilst arguably ethically lamentable, this shortfall may actually be costing Australia financially. Does Australia need to reform its information privacy protection further or can we afford to allow the international information market to develop without our full and free participation?

Keywords: Information Privacy International Standard Legislative Reform.

What is Personal Information?
As Australian businesses begin to use and trade in personal information, many unwittingly do so in breach of either our own privacy protection measures or those in other countries. This is largely due to a poor understanding of what personal information is and how it is regulated.

Personal information is generally understood to be information such as name, date of birth and address. This definition fails to include data such as habits (such as shopping, eating, or drinking), movements (including toll roads, surveillance cameras, or even web browsing) and generally, any information that can be linked in any way with a given individual (such as friends or beliefs). When broadly defined in this manner, personal information comprises a significant percentage of organisational databases. As greater controls are placed on how such information can be gathered, stored and used, the cost to organisations will similarly increase.

How is it Regulated?
Historically Western European and Scandinavian countries led the information privacy protection charge in the 60’s and 70’s with many other countries following suit, including Australia, throughout the 70’s, 80’s and 90’s. Slane, B (2001) notes

Generally countries with low levels of e-commerce and/or technology tend to offer less protection whilst more technologically advanced states offer increasingly strong protection. This increase in protection is usually due to a number of pressures. The first and foremost is consumer concern. Such concern is the result of increasing collection and use of e-data by business and government. The second and perhaps more surprising pressure, arises from the private sector (Cant, 2001; Reidenberg, 2001; Slane, 2001). This pressure is twofold with organisations trying to improve B2C relations and augment B2B trade in personal information. Strong privacy protection measures reassure consumers whilst facilitating free trade with other jurisdictions. Thus the end result is usually stronger local and national privacy protection laws. This progression can be observed in a number of jurisdictions including Canada and New Zealand. Australia also appears to be following the same path, albeit at a slower pace.

Not all countries follow suit however. The most notable exception is the United States which offers very little privacy protection, concerned with specific issues such as health care and personal finance. The U.S. has so far resisted the international trend by brokering a deal with the E.U. to allow free trade without meeting the E.U. standard. Even so, there are real doubts that the Safe Harbour agreement can endure.

An American law professor, Joel Reidenberg (2001) told the U.S. congress that although its size and commercial bargaining position had enabled it to broker the ‘Safe Harbour’ deal with the E.U., it was ultimately doomed. He commented that although the deal facilitated trade between the E.U. and subscribed U.S. organisations in the short term, it was not a long term solution.

Reidenberg is not alone with many others drawing the same conclusion, including the New Zealand Privacy Commissioner (2001). Both Reidenberg (2001) and Featherly (2001) suggest that despite the Safe Harbour Agreement, there is mounting pressure for the U.S. to develop a national standard. Indeed, even if national privacy laws are not enacted, individual states may do so on their own. If so, Thibodeau (2001) and Slane (2001) argue that this will force national legislation into place.

Of course there are others that argue to the contrary. The above conclusion is strongly rejected by many U.S. lobby groups who assert that self-regulation and the Safe Harbour Agreement will suffice. Unfortunately for these lobbyists, the weight of evidence is against them. The number and frequency of privacy bills being put forward (often exceeding one hundred at a time) at the state level suggest that privacy reform is inevitable.

Other countries with less bargaining power or will to dictate their own terms are slowly amending their own legislation in favour of the E.U. standard. Slane (2001) notes that smaller countries cannot expect to broker individual deals with the E.U. Often compared with Australia, Canada had tried self-regulation but had failed the
E.U. ‘adequacy test’. In 2000, it finally succumbed and amended its legislation to meet the E.U. standard.

Like Canada, New Zealand has also recently amended its legislation to offer ‘adequate’ protection under the E.U. directive. The 2001 Australian privacy amendments were in part modelled on the 1995 New Zealand Privacy Act, which itself failed to meet the E.U. standard. In 2001, the New Zealand Privacy Commissioner commented that the Australian legislation would also fail the adequacy test and urged it to consider further amendments.

As new personal information markets arise throughout Asia, so too are privacy reforms. Many Southeast Asian and pacific nations are enacting or amending their own privacy laws in an effort to meet the E.U. standard. These countries include Thailand, Hong Kong, Malaysia and Micronesia. If Australia is to continue using and trading in personal information in the Asia Pacific region, it will need to follow suit.

Currently Australia is not alone and there are many countries that fail to meet the E.U. standard, including some member states of the E.U. itself. This position is slowly changing however as more and more countries seek to gain free trade status with the E.U. If this progression continues, it will only be undeveloped countries and the U.S. that will remain outside the E.U. free trade zone. Can and should Australia remain outside that zone as well?

Slane (2001) points out that Australia, Canada and New Zealand have all already devoted both time and money to trying to meet the E.U. Adequacy test. Both Canada and New Zealand have attained that goal, will Australia and if so, when?

**Why Change?**

Australia is already facing mounting pressure to further improve its privacy protection. Indeed, late last year, despite the amendments, the EU held that Australia failed the E.U. ‘adequacy test’ (Slane 2001). The Australian Attorney General (2001) argues that Australia meets the E.U. standard and that the E.U. has misunderstood our legislation. Unfortunately for the Attorney General, even the Australian Senate Legal and Constitutional Committee (1999) agreed that despite the then proposed amendments (now enacted) Australia’s privacy protection would not be up to the E.U. standard.

It should be noted that this finding does not prevent individual Australian organisations from trading with EU organisations. Rather, as Slane (2001) points out, those organisations must first meet the EU standard – a cumbersome and expensive accreditation process when compared with the alternative of an adequate national regime.

It may be argued that Australia offers a pragmatic ‘user pays’ system whereby only those organisations that wish to trade with the E.U. need meet its standard. Although meritus, this approach does not really save any money. Each time Australia’s privacy laws are amended, organisations must invest significant amounts of time and money in complying with those new amendments. The cost of this cycle of compliance is actually greater than meeting the highest standard in one step. Would we not be better
to meet the EU standard now instead of slowly amending our legislation time and
time again?

If privacy regulation follows the path of many other international legal issues, it is
likely that an international standard will emerge. The logical question becomes, what
will that standard be? Will it favour the less regulated US approach or will it favour
the more protective EU model? The slow shift in local privacy laws in favour of the
E.U. standard, combined with the increasing economic might of the E.U. suggest that
if a standard is to emerge, it will closely resemble the existing E.U. standard. Even if
this is not the case, a de facto standard may emerge by virtue of pressure from the
E.U. and once again, it will be closer to the E.U. model than the U.S. one. Indeed, the
New Zealand Privacy Commissioner (2001) concludes that an international standard
or at least set of principles is likely. Slane (2001) points out that many Asian and
Pacific nations are attempting to meet the E.U. standard. He goes on to say that failure
to meet the standard will result in loss of income and trade opportunities.

Countries unable to dictate their own terms, such as Australia, will ultimately benefit
from meeting the standard sooner rather than later. Many may be tempted (as
Australia and Canada were) to allow business to self regulate, but this may prove
inadequate and costly in the long run. These costs may be measured both in terms of
direct financial cost and loss of opportunity.

Compliance Cost
The compliance cost to business does not bear a direct correlation with the standard
set. Rather, the cost to business comprises a base cost for compliance assessment and
an additional implementation cost. Although the implementation cost may vary
depending upon the standard of protection set, it is not a linear relationship. Thus the
relative cost to business in Australia is arguably greater than in other countries that
initially enact an ‘adequate’ (or E.U. standard) of privacy protection.

The compliance cost is can be measured in other ways as well. Although individual
companies may meet the E.U. standard, the cost of doing so is significant and inhibits
trade overseas. This is not the only transjurisdictional issue however. Even those
organisations that use or store personal information across jurisdictional borders may
suffer financially. The ban on the transborder flow of personal information is not
confined to trade alone. It also includes the movement of personal information within
a company. For example, a company that stores personal information (such as a
customer database) in another jurisdiction may be in breach in both jurisdictions.
Australia already bans such transborder flows and thus this is not hypothetical, but a
very real problem for many organisations.

Opportunity Cost
The opportunity cost is also significant in its own right. Currently most Australian
businesses do not trade overseas. Traditionally geography constrained, electronic
commerce has removed many geographical barriers and facilitated trade between
different countries. In its place, one of the major obstacles to international trade is
now regulatory. In the case of personal information, the differing standards of privacy
protection are posing very real barriers to trade. In Australia’s case, organisations that
may have used personal information to increase revenue or developed ties with
overseas counterparts cannot easily do so. This cost is not yet apparent as most
Australian businesses to not operate overseas. Whether this will remain the case is yet to be seen. Regardless, there is little doubt that Australia’s failure to meet the E.U. standard has and will continue to have, a dollar value in lost trade opportunities.

Conclusion
Australian privacy protection is not insignificant. When viewed in a global context, Australia offers better protection than most. Unfortunately whether rightly or wrongly, it still fails the E.U. adequacy test. Unlike the U.S., Australia cannot dictate its own terms and as other countries fall into line with the E.U. standard, Australia will be left behind.

Some argue that the cost of compliance with the E.U. standard is not worth the benefits it would engender. This argument is flawed however. Each time Australia amends its privacy legislation, the cost to Australian businesses is not unduly greater than it would be to meet the E.U. standard in the first place. Furthermore, as other countries continue to meet the E.U. standard, the direct and indirect cost to Australian businesses will grow. Moreover, if an international standard does emerge, Australia may need to bring its own privacy protection measures into line. Viewed in this light, Australia’s procrastinations seem counter productive and decidedly isolationist. Ultimately, it may be Australian organisations that force change rather than traditional consumer issues.

References
Designing Ethical Systems for Electronic Commerce

Shona Leitch¹, and Matthew Warren²

¹ School of Information Technology
   Deakin University, Australia,
   E-mail: shona@deakin.edu.au;

² School of Information Technology
   Deakin University, Australia,
   E-mail: mwarren@deakin.edu.au;

Abstract

Ethics is an important element in all aspects of computing, but proves to be a real problem in the development and delivery of electronic commerce systems. There are many aspects of ethics that can affect electronic commerce systems, but often research is focused on the ethics after the Electronic Commerce system has been implemented, focusing on issues such as trust, privacy and disclosure. This paper will discuss how ethical matters can affect the design of Electronic Commerce systems and how a framework designed for Electronic Commerce can be used to create and deliver effective, ethical Electronic Commerce systems.

Keywords: E-Commerce, Ethics, framework.

Introduction

There is a lot of talk especially in the popular press as to the virtual explosion of e-commerce over the past few years, however many reports indicate otherwise. Or at least indicate that this ‘explosion’ is only taking place in certain sub-sections of the e-commerce industry.

According the National Office for the Information Economy (NOIE, 2001) over a half of Australia’s population has a personal computer in their homes and 35% have Internet access. Along the same lines, most medium-sized businesses and over 80% of what is termed small business use personal computers. ‘Over 35 per cent of all businesses have an online presence—a comparative business advantage that translates into Australia being consistently rated in the top ten nations globally for its e-commerce environment.’ However this does not necessarily mean that Australia is performing and using e-commerce well, a web presence does not necessarily mean ‘electronic commerce’ either. And further enlightenment from NOIE comes from the following statement:

‘Five per cent of Australian adults shopped via the Internet in the 12 months to February 2000, and 74 per cent paid for their purchases online. Take up rates of other kinds of e-commerce—such as telephone banking and electronic funds transfer—were even higher.’

(NOIE, 2001)
The aim of the research was to produce a workable framework, which incorporates parts of previously validated systems design methodologies that encompasses all the needs and requirements of users in an e-commerce environment. By using a mixture of methodologies, we are able to also consider the fact that the system is designed ethically.

One concern that we need to consider is that the ‘systems’ part of an ‘information system’ (including e-commerce systems) represents a way of seeing the set of interacting components, such as:

- People (e.g. systems analysts, users)
- Objects (e.g. computer hardware devices)
- Procedures (e.g. those suggestions made in an IS development methodology) (Avison, 1999)

Often in systems design, the developers focus on the objects, i.e. making the most technologically advanced system. In the case of E-Commerce B:C systems, the users are focussed upon in an attempt to sell more product and market more effectively, and often in a way that encourages unethical practices when designing systems rather than producing a system that is in the users best interests.

**Project Success and Failure**

At the present time Internet businesses have access to a wide audience with 11% of Australian households with Internet access and over 40% of U.S households. Therefore, there must be other reasons why people do not utilise online web retail or undertake B:B transactions.

E-Commerce poses unique design issues:

- Fast development time
- Lack of expertise in systems design means the need for an easy to use method
- High failure rate, due in part to poor systems analysis and design
- Heavy user considerations, particularly in B:C

One example of an E-Commerce failure was the UK online retailer, BOO.com. Who even though had a potentially huge client base failed to capitalise on this due to poor systems design and web design and a lack of consideration of users:
Figure 1 – Website of BOO.com

The reason for failure was that a large proportion of its potential market was unable to use Boo's site because the website design was too advanced for most computers and access frustratingly slow (BBC, 2000). Other reasons for BOO.com failure included:

- the site could not be seen by people who use Macintosh computers.
- it used lots of graphics, pop-up windows and 3-D images that only those with a 56k modem could see it without waiting minutes for it to load.
- the site was very difficult to navigate around. Shoppers could get lost and find no way back to their starting point.
- BOO.com was funded to the tune of some A$180m (£80m). Boo's problems also centered on its inability to build up numbers of buying customers fast enough, to generate revenues to offset steep set-up costs.

It is probable that a use of systems analysis techniques could have overcome these problems.

“Firms that cannot deliver - either because their web site is poorly designed or because their distribution system is not up to scratch - are bound to fail” (BBC, 2000)

The concerns of system success and failure are very real. Within any new computer system, a great deal of time, effort and monies are invested, with little guarantee of there being success at the end of the project. Companies that employ system designers, or model, analyse and plan their system would seem to have the best chance at achieving a truly helpful, workable system.

The rise of the Internet as a locus of business is changing marketing, for instance. It makes possible one-on-one marketing by tracking the customer, recording his or her
preferences and proclivities, and presenting the customer with products that he or she is likely to want to buy. High street stores, similarly to TV ads, have to generalise their marketing to an average consumer. The Internet makes it possible for a company to design a system that lets each consumer have an individual fit. This can be done to aid the user, by remembering certain likes and dislikes, but more often that not, it is done unethically to entice people to buy things they do not need through a huge purchase driven experience.

By incorporating a participational aspect to systems design, and including the user at this stage it is very likely that a system would be developed that is more ethically sound to those B:C E-Commerce customers.

But other studies have identified advantages in using a participational approach. Adams (1984) found that:

- Staff/users have ideas which can be useful;
- effective upwards communications are essential to effective decision making at the top;

It is clear that human participation in the design of electronic commerce systems would be innovative and useful. This has been widely reported through anecdotal evidence as well as experimental studies.

“Web-site usability is better than it was a few years ago, but there is still a long way to go, according to a recent e-retail site-usability survey conducted by Nielsen Norman Group. Retailers should take a fresh look at their Web stores. Approach them as a shopper would, and look for flaws that could raise customers' blood pressure.”

(Scheraga, 2002)

“The redesign effort at Egreetings to improve the number of online greetings sent by users is discussed. Whenever a website has a major makeover, it is normal to expect that users will encounter difficulties and some traffic loss will happen. In this case, traffic statistics actually improved as well as the overall ratio of cards sent per visitor. The time and effort spent in learning about how the site's users think about online greetings was a key factor in this successful outcome.”

(Farnum 2002)

**Framework Overview**

The authors have developed a framework which could be used for the design of E-Commerce systems, focusing upon user requirements. The issues of ethical design can be resolved by ensuring that users are key stakeholders in the design of the systems that they will be using. The stages of the framework are:
Stage 1 – Strategic and Business Evaluation

1. Assess present level of E-Commerce against criteria.
   Criteria:
   - Level 1 – No web presence
   - Level 2 – Have web presence (website with contact data etc)
   - Level 3 – Have web presence and use B:B
   - Level 4 – As level 3 and use B:C
   - Level 5 – Use both B:B and B:C
2. Decide future level of E-Commerce using the above criteria.
3. Create detailed plan for business/systems development
   - Set up project team
   - Identify key business activities (BSP)
   - Develop a formal plan (objectives, goals, resources) (Lederer and Mendelow, 1989)
   - Link E-commerce plan to business plan
   - Perform cost benefit analysis – identifying tangible and intangible benefits
   - Prepare for change
4. Perform feasibility and SWOT analysis
   - Define information systems outline
   - Select feasibility options (SSADM)
   - Identify strengths, weakness, opportunities and threats
   - Create feasibility report

Stage 2 – Systems Analysis and Design

1. Create rich pictures from level 2 and 3 of stage 1 to create a conceptual model of system and user requirements.
2. Apply a participational Approach to level 1
   - Use a cross census of users to discuss the rich pictures
   - Reflect on outcomes of discussions
   - If possible, assess e-commerce user requirement, also using the participational approach (perhaps with a pilot group of Internet users)
   - Reflect again on these outcomes
3. Create final rich picture

Stage 3 – Systems E-Commerce Design

1. Undertake process modelling
2. Assess technical considerations
3. Assess security considerations

Stage 4 – Implementation

1. Undertake the physical implementation of the web-site.

Stage 5 – Post Implementation

1. Using the participational approach, discuss and reflect on issues arising through implementation.
Stage 1 of the framework could be compared to traditional systems analysis and design methods that implement feasibility studies (SSADM), requirements elicitation or other problem identifying skills. Although part of the beginning of this framework aims to also provide some insight into the feasibility of an e-commerce project, it also provides a much deeper, strategic and business evaluation than using just one of the above. From current statistics of organisations use of feasibility studies, two thirds of organisations did not conduct / sometimes conducted a feasibility study (Leitch, 2001). It is also believed that the inclusion of a feasibility aspect of the design, will encourage companies to assess their business function and customers wants, needs and expectations. The benefits of feasibility studies are widely reported, and therefore it was decided to include an ad-hoc one within this framework.

Initially it was decided that a developer would first have to decide at what ‘stage’ of E-Commerce the organisation was at. This is deemed to be important, as many e-commerce businesses as they define themselves are little more than an online advertisement. Therefore by categorising themselves, it is easier to proceed through other levels of E-Commerce development. As at this initial level, it is suggested that the developer/analyst also decides to which level the organisation wishes to pertain through the development of the present project.

A large amount of focus on the new framework for E-Commerce was put into the strategic and planning stages, although this is not aimed at taking up a large amount of a potential analyst’s time, it is perceived to be straightforward enough to do in a timely manner whilst still providing a developer with enough information and safeguards to know that their project has merit. Therefore, in the 3rd step of stage 1, it is suggested that the developers do a number of formal steps to aid in the proposed project.

In stage 2 of the proposed framework, a number of traditional steps were used, in order to provide the best possible analysis stage for the area of e-commerce. The needs of e-commerce in terms of systems analysis and design are not adequately covered in any of the major methodologies and frameworks that have been written so far. However parts of these methodologies and frameworks have aspects that are relevant and useful to E-Commerce design. The use of a form of rich pictures (Checkland, 1981) will both incorporate the users of a system, as well as providing an easy to understand and relate to method of eliciting and discussing information between the designers and other stakeholders. It is suggested that ETHICS (Mumford, 1983) is used as the way to conduct these meetings. This information can then be taken by the designers and created into simple DFD style diagrams for the coding stage. Again post-implementation will make use of a participational approach to assess the new system.

It is not being suggested that designers follow methodologies closely, this framework is suggesting the best methods to use to create a new e-commerce system, and recommends the principles of some tried and tested methodologies are implemented, but as the need for a fast creation time is paramount, then the full and detailed layout of each type of methodology will not be followed.
Conclusion

The results of this unique research, with the analysis of the most commonly utilised systems analysis methodologies as well as considering the wants and needs of organisations creating E-Commerce solutions, will allow for the production of a framework capable of assisting in more effective, successful and ethical E-Commerce systems.

References


BBC (2000) ‘From Boo.com to Boo.gone’
http://news.bbc.co.uk/1/hi/business/753782.stm [accessed 14/08/02].


Farnum, C; American Society for Information Science. Bulletin of the American Society for Information Science, Washington; Jun/Jul 2002; Vol. 28, Iss. 5; pg. 10, 4 pgs


Scheraga, D. (2002); Chain Store Age, New York; Jul 2002; Vol. 78, Iss. 7; pg. 60, 1 pgs.
Workplace email: surveillance, privacy and ethical protocols

Paula Roberts

School of Communication, Information and New Media
University of South Australia
Paula.Roberts@unisa.edu.au

Abstract
The conversational nature of email places its function and style somewhere between a letter and telephone conversation but without the legal privacy protection of either. Mainly used in workplaces, e-mail’s technical infrastructure allows easy perusal and archiving of messages by employers and systems operators. Debates continue regarding employees’ rights to email privacy and employers’ rights to monitor email. The privacy/transparency dichotomy represented by competing interests of employee and employer extends beyond legal rights to matters of distributive justice, which suggest an ethical base for email protocols, and for establishing trust between employee and employer.

Keywords: Email privacy; distributive justice; workplace trust

Introduction
This paper discusses the erosion of workplace privacy as surveillance technologies become pervasive in the workplace. Inexpensive to establish and hidden from the employee’s view, they enable closer and more continuous monitoring of an employee’s activities than the capacity of a human supervisor to undertake.

The main focus of the paper is employees’ use of institutional e-mail communications and their unrealistic expectations of privacy from the gaze of management. This naivety has come about through the nature of email and its seeming similarity to traditional oral and print communications, and the legal protection afforded these older media. For example, copyright legislation protects the printed word, and telecommunications legislation prohibits the hidden recording of telephone conversations.

However, employers have rights (although their legality is questionable) to monitor employees’ email usage in order to protect the organization against possible litigation brought about by the inappropriate employee use of email technology for the purpose of transmitting defamatory or abusive messages. As well, it is argued, surveillance is necessary to prevent confidential company information being transmitted to commercial rivals.

The employee-privacy/employer-transparency dichotomy relates to theories of distributive justice outlined by Introna (2000) who argues that Rawls’ system of
justice for the individual, rather than the utilitarian view of sacrificing the interests of
the few for the betterment of all, should prevail in matters of workplace surveillance.

This dichotomy presents an important task for organizations to produce protocols for
workplace email usage which acknowledge the competing rights of employee and
employer.

**Employee rights to workplace privacy**

Workplace monitoring is made easier by surveillance technology which is “cheap,
implicit and diffused” and “more ‘close’ and continuous than any human supervisor
could be” (Introna, 2000: 33). Introna (2000: 34) reports that formal surveys such as
Lyon (1994: 131) found that, in 1990, up to one million jobs in Britain were subject to
security checks. In 1993 in the United States, estimates by the International Labor
Office suggested the electronic monitoring of some 20 million employees, and a 1999
survey by the American Management Association revealed that 45% of major U.S.
firms “record and review” their employees’ phone calls, computer files and email.
These surveys may not indicate the true extent of workplace surveillance because
organizations are unlikely to reveal their monitoring of employees.

In the nineties, management increasingly needed to justify its surveillance practices,
but, it can now be argued post September 11, that society in general may come to
accept an increased level of personal privacy invasion, thereby opening the way for an
increased monitoring of employees.

Research indicates that workplace surveillance damages staff morale and increases
workers’ stress, “leading to resentment and undermining trust between employee and
manager”, Gannon-Leary (1999: 168). That privacy is an essential human need has
been argued, (amongst others) by Benn (1984), Gavison (1984) and Johnson (1989).
More specific for the scope of this paper, privacy in the information age has been
Spinello (2000: 11) defines privacy as the limitation of others’ access to an individual.
Privacy has three key elements: secrecy, anonymity, and solitude. In particular,
secrecy (or confidentiality) involves limiting the dissemination of knowledge about
oneself. Clarke, (1988) outlines the erosion of employees’ informational secrecy as
they are subjected to what he terms “dataveillance”, that is, the systematic use of
personal data systems to keep track of an individual’s actions or communications.

Benn (cited in Spinello 1995) contends that even covert watching of an individual,
which may not cause direct injury, is nonetheless “disrespectful and wrong”, and is
objectionable because it “deliberately deceives a person about his world, thwarting for
reasons that cannot be his reasons, his attempts to make a rational choice.” Similarly,
Gould (cited in Spinello 2000: 12) observes that “privacy is a protection against
unwanted imposition or coercion by others and thus a protection of one’s freedom of
action.” Spinello (2000: 12) argues that, as privacy diminishes for an individual, he
or she becomes “more subject to the manipulation and control by others” and “more
inhibited and timid about the pursuit of our goals and activities.” He quotes Foucault
(1979: 200) who likens this phenomenon to the “panoptic effect” that most prison
systems seek to achieve, whereby the inmate feels that he or she is in a “state of
conscious and permanent visibility that assures the automatic functioning of power.”
**Nature of e-mail and employee expectations of privacy**

Email, in a few short years, has become a major business and communications tool. Lee (1996: 275) points to the origins of email in the older conventions of typography and letter and memo writing, however, email diverges significantly from pre-electronic writing by incorporating elements of oral media such as telephone conversations and face-to-face communication. These older print and oral media have been accompanied by legal rights, for example, copyright of the written word, and oral privacy protection, such as the prohibition of “phone-tapping”. There has been first an assumption and now an increasing uncertainty amongst email users that this same legal protection of their privacy in the old communications media applies to their email communications.

Privacy notices at the bottom of e-mail messages, (such as samples shown below), vary considerably between individuals in an organization, and between organizations. Their tentative tone reflects the senders’ uncertainties regarding their email privacy.

The first example is from a university academic, and the second from a university vice chancellor:

- This email message is intended only for the addressee(s) and contains information which may be confidential and/or copyright. If you are not the intended recipient please do not read, save, forward, disclose, or copy the contents of this email. If this email has been sent to you in error please delete this email and any copies or links to this email completely and immediately from your system;

- Please Note: This email is intended for the addressee(s) only. Should this email be received in error by a person or company other than those intended, the contents of this email are CONFIDENTIAL and must not be released or used by a person or company not authorized to do so.

The first privacy notice reflects a naivety which is common amongst email users regarding the deletion and continual storage of email messages. Sipior and Ward (1996) remind us of an infamous example of misplaced belief in deleted messages which occurred in the Iran-Contra investigations conducted by the U.S. Congress, when messages between Oliver North and John Poindexter were retrieved from White House backup tapes. North said in his testimony, “We all sincerely believed that when we sent a PROFS message to another party and punched the button ‘delete’ that it was gone forever. Wow, were we wrong.”
The privacy notices set out above refer to confidentially, and the first refers also to copyright. Confidentially cannot be assured when a message is received in error, and the sender’s legal copyright is uncertain in Australia, although possibly more secure in some jurisdictions in the United States (Halbert, 2001). Intriguing also is the vice-chancellor’s notice regarding privacy which might apply neither to the employees’ nor the vice-chancellor’s email.

The legal status of e-mail privacy is uncertain. In the United States, for example, Griffin, (cited in Sipior and Ward, 1996), reports claims arising from common-law invasion of privacy are generally unsuccessful with respect to email monitoring, primarily because such monitoring does not affect any legally recognized individual privacy interest. As Sipior and Ward detail, the United States Electronic Communications Act (1986) while “not afford(ing) significant privacy protection to employee email communications” did offer some protection. This related to the “Prior Consent” clause which might protect employers against risk of liability by their notifying employees that employee email might be monitored.

It was thought that the Privacy for Consumers and Workers Act (introduced in 1993, but awaiting ratification at Sipior and Ward’s time of writing in 1996) had the potential to “significantly restrict an employer’s ability to legally monitor employees’ email”. The Act required that employers:

1. Provide advance written notification to employees if email messages or computer keystrokes are to be monitored;
2. Notify employees of any monitoring policies; and
3. Disclose entry into an employee’s hard drive after the fact. (Sipior and Ward, 1996)

Johns (1995) argues that the obligation on employers to supply written policy statements regarding the monitoring of all communication using company equipment has also served the useful purpose of removing a misplaced employee expectation of email privacy.

Email surveillance and employer expectations of transparency

Written policies regarding employee monitoring, designed to protect employees, in effect have become a “double-edged sword”, for as Dichter and Burkhardt, (cited by Introna, 2000) point out such policies imply prior consent from employees for workplace surveillance, and implied consent is recognized by U.S. law. Thus, employers who notify employees that their telephone or email communications are likely to be monitored will have the implied consent of their employees for this to happen (Santarelli, 1997). In this respect the legal balance has swung away from the intent to protect the privacy of employees, and a power imbalance has emerged in the application of what might have been a democratizing telecommunications tool in the workplace. As Gannon-Leary (1999: 165) reports, many U.S. companies have now declared “sovereign power over electronic communications that originate in the workplace.”
It is not disputed that employer expectations of transparency reflect a management need to monitor communications which might involve employee breaches in commercial confidentiality, and to protect employers from possible litigation arising from employees’ email communications if they contained defamatory, abusive or pornographic content. But, as Introna (2000) argues, the important issue here is that, apart from Sweden, there is little enacted legislation in western democracies and, therefore, no legal obligation on employers to ensure that workplace monitoring is not “invasive, unfair or stressful.”

**The privacy/transparency dichotomy and distributive justice**

If we accept both employees and employers have rights regarding privacy and surveillance, how might fair outcomes be achieved for both? Introna (2000) argues the issue is a matter of ‘distributive justice’, that it is necessary to establish a framework for distributing the rights of privacy and transparency between the individual employee and their employer in a way which is fair to both. It is generally accepted the best interests of the individual are served when they have control over their privacy, to ensure freedom from the “inappropriate judgement of others” (Johnson, 1989). For commercial advancement, it can be argued that the institution requires control over surveillance, that is, subjecting all employees to reasonable scrutiny.

In view of this conflict between the individual employee and the employer, Introna (2000) suggests that Rawls (1971) framework of justice as fairness, in opposition to utilitarianism, is a useful starting point. In the case of email surveillance, utilitarianism would place no restrictions upon the subordination of some interests (the employees) to those of others (the employers), except that the net outcome be good, that is, the protection of the organization. Rawls argues that a theory of justice cannot allow disadvantages to some (the employees) to be justified by advantages to others (the employers).

As Introna explains, in respect of workplace surveillance, there is danger in setting the supposedly “limited cost of the loss of individual privacy against the enormous economic benefit to the institution of securing effective control over productive resources.” Such utilitarian arguments can trivialize the individual employee’s claim to privacy in the face of the economic prosperity of the whole organization. Introna argues that, “it is exactly this utilitarian type of logic that continues to limit the legitimacy of the individual’s claim to privacy in the workplace”.

**Establishing fair protocols for workplace email usage**

Prevailing organizational practices with regard to workplace surveillance which favour the employer both in data gathering and control are unfair to employees.

Using Introna’s theories regarding a fair distribution of privacy and transparency rights would suggest that protocols for workplace email usage must acknowledge:

> the right of the employer to monitor individuals’ activities with respect to the use of the organization’s communications technologies, and to use the data collected in a fair and reasonable way for the overall good of the organization as a whole.
that the employee has a legitimate claim to limit surveillance of their email communications. The employee also has a right that management justify all monitoring of email traffic and ensure that the data collected will be used in a fair and reasonable way.

How protocols for email communications might be established is another problem. The solution might lie in the negotiated enterprise bargaining agreements used increasingly in Australia. These agreements cover salary and workplace conditions as part of the employment contract between employer and employee. Renewed periodically after protracted and sometimes bitter negotiations between employer and nominated employee-representative bargaining groups, these workplace agreements nevertheless provide an opportunity for informed discussion and bargaining with respect to a range of employer/employee issues. It is most likely that the electronic monitoring of employees, and in particular the surveillance of e-mail communications has so far not been included in these negotiations.

The reasons for this omission are several. Firstly, electronic monitoring is a hidden form of workplace surveillance which an organization is unlikely to make evident unless this becomes necessary, for example, in an investigation of a dispute between an employer and an individual employee (Bjerklie, 1993; Sipior & Ward, 1995; Spinello, 1995; Gannon-Leary, 1999). Secondly, a protocol (if one exists) for the use of an organization’s information technologies may be limited to a brief general statement about expected standards of employee behaviour (and student behaviour in the case of universities) when using IT systems. Finally, the imbalance of power between management and employees has become more extreme in Australian workplaces in recent years as democratic management styles have declined and given way to leadership which has become progressively more autocratic. This increasing power imbalance has been accompanied by a reduction in communication, and diminishing trust between management and employees, which has rendered more difficult the establishment of fair monitoring of employee performance.

**Conclusion**

In a post September 11 world the potential for workplace surveillance has increased, as has the conflict between the individual right to privacy in the workplace and the institutional right to transparency in respect of employee behaviour.

Introna (2000) contends that the issue of workplace surveillance must be negotiated along the lines of competing but equally legitimate claims for privacy and transparency. With this understanding in place, “the possibilities for the individual ‘to resist inappropriate workplace surveillance’ increases dramatically.” Introna believes that, with Rawls’ theory of justice as a foundation for negotiating a ‘fair regime of workplace surveillance’, monitoring should be avoided unless explicitly justified by the employer.

Protocols which clearly set out joint responsibilities of employer and employee to ensure fair usage of communications technologies appear the best chance to establish an equitable regime for email use which avoids diminishing employee privacy and encourages workplace trust. The challenge for institutions now is to set up the intellectual and organizational resources to ensure that email surveillance, if and when it is appropriate, becomes fair and stays fair.
References


The Inadequacy of Existing Ethical Codes for On-line Research: 
A matter of Informed Consent

Paula Roberts and Jenny Webber

School of Communication, Information and New Media 
University of South Australia 
paula.roberts@unisa.edu.au

School of Communication, Information and New Media 
University of South Australia 
jenny.webber@unisa.edu.au

Abstract
Researchers have been quick to tap the rich data source for social science represented by on-line discussion groups. However, ethical codes designed for face-to-face investigations are inadequate for cyber-research in respect of gaining the informed consent of electronic participants. As well as problems of constantly changing membership, the anonymity of group members which protects their privacy also masks personal demographics such as age and intellectual capacity essential in gaining informed consent. Existing ethical codes present problems for institutional ethics panels who might have difficulty in judging both the validity and the ethical soundness of proposed cyber-research projects.

Keywords: Cyber-research; Ethics codes.

Introduction
On-line discussion groups allow widely-distanced people with shared and often intensely private interests to communicate with one another for information sharing and mutual support (Sudweeks, et al. 1998). These groups provide opportunities for social scientists to study the dynamics of electronic interactions, and to collect data from distanced participants with ease and speed, more economically than similar research in the physical world. These factors have encouraged a steady increase in Internet research, both quantitative surveys and ethnographic studies involving participant observation (Reid, 1996; Waskul and Douglass 1996).

The electronic research medium, whilst offering huge potential for extending scholarship raises issues about conducting research with human subjects (Schrum, 1995; Childress and Asamen, 1998). For example, the Internet allows both researchers and their subjects to assume anonymous or pseudonymous on-line identities which obscure details such as gender, age, physical and mental ability, demographics which might be important to the investigation (Kendall, 1999).

There are two major and distinct sections in the literature in respect of cyberspace anonymity, one which relates to Internet commerce and the other to the social and voluntary practice of Internet communication. For the purposes of this paper, the latter has most relevance, particularly the anonymity practised in on-line self-help groups
(for example, Waskul and Douglass, 1996). The descriptors ‘anonymous’ and ‘pseudonymous’ are not always clearly defined in the research literature, however, Marx (1999) provides a useful definition in suggesting that anonymity relates to the purposeful non-revelation of personal characteristics, while pseudonymity relates to the adoption of another cyber identity (e.g., van Gelder, 1996).

In addition to problems posed by anonymity for research validity, the changing membership in Internet communities creates difficulties in obtaining informed consent from subjects, some of whom may be minors (Schrum, 1995; Reid, 1996), and the uncertain distinction between the public and private domains causes confusion and possible harm for many subjects who hold illusory and unrealistic expectations of privacy (Reid, 1996; Witmer, 1998).

These significant differences between virtual and physical research environments raise questions about the interpretation and applicability of current research ethics policies, such as the Commonwealth of Australia, *National Statement on Ethical Conduct in Research Involving Humans* (1999) which, like similar international research codes, rests on the principles of integrity, respect for persons, beneficence, and justice.

The first principle, *integrity*, relates to the honest and ethical conduct of research, and dissemination of its results. The second, *respect for persons*, requires that participants are treated as autonomous agents, and affirms that persons with diminished autonomy (such as the young and the physically and intellectually impaired) are entitled to special protection. This principle is reflected in research practice as the process of informed consent, whereby the risks and benefits of the research are disclosed to the subject or their guardian before the investigation can proceed. The third principle, *beneficence*, involves maximising the possible benefits for the subject, while minimising the amount of possible risks and harm. The last, *justice*, seeks a fair distribution of the burdens and benefits associated with the research.

These principles, judged as adequate and appropriate for research involving human subjects in the physical world, require redefinition and extension for Internet research, as becomes increasingly apparent in case studies of research with on-line communities where the social and technical complexities of the medium may have unexpected and unwanted outcomes (Thomas, 1996; Witmer, 1998; Denzin, 1999).

**Case Studies of Internet Research**

Thomas (1996) reports an Internet research project which went ethically awry. The improprieties of this quantitative, undergraduate study were many, but, in summary, the project involved an analysis of the text descriptions of erotica files taken from electronic bulletin boards, including an analysis of Usenet postings and readership which was obtained, without consent, from the private files of users on a university computer system. At the researcher’s request, (but in breach of ethical privacy standards), system operators collected other data and provided confidential demographic details, that is, age, sex, faculty, staff, student and department. Further details were taken from usage statistics of the university computer site, allowing tracking of some four thousand individual users ‘who accessed pornographic and/or non-pornographic Usenet newsgroups once a month or more’.
Thomas comments that, obvious lapses aside, such as inadequate supervision, the problems in this project related primarily to the social and technical aspects of the on-line environment. These users showed naive expectations for anonymity, and lack of awareness that the personal information they generated by their on-line activities was traceable and stored by computer systems without their knowledge, remaining there for years possibly at the mercy of ill-defined privacy protocols (Thomas, 1996; Witmer 1998). Of greater significance was that the research was conducted in a clandestine manner without first gaining informed consent from the unwitting ‘participants’ of this research study.

Thomas’ complaint referred to a quantitative study, but it is ethnographic research in general, and studies involving participant observation in particular, which cause most risk for the privacy of members of on-line discussion groups.

Even cyber-research which has aimed to be ethically impeccable can have unexpected, harmful consequences, as is described by Reid (1996) who conducted a participant observation study of virtual communities established for therapeutic, self-help purposes. Reid reports that despite using existing ethics protocols to ensure her research was undertaken in an appropriate manner, the ‘research has been a factor adversely affecting at least one of the communities’. On reflection, Reid outlines the problems created by the blurred distinctions between private and public data, and the difficulties in gaining informed consent from a changing population of users. Reid notes also (because of the group’s changing membership) the need to announce regularly that she was a researcher/member could not be done without disrupting the group’s normal social flow, and that to obviate this ‘some measure of deception, or non-disclosure, (on the part of the researcher) was inevitable’.

More critical problems of consent and disclosure occurred in a group designed as a support centre for survivors of sexual abuse. Reid points out that she could have, with the full consent of those involved, published extracts ‘that revealed deeply personal information about these people’s lives and experiences’. Reid chose not do this, but notes that the lack of inhibition in on-line communication, and the allure of self-revelation, may lead group members to public and harmful exposure. Despite her care, Reid believes the group suffered from the effects of her research, and from the attention of subsequent researchers. The group survived only by restricting its membership to genuine sexual-abuse sufferers and by restricting its use of the technology, a trade-off which made the support group safer, but less open.

Outcomes for cyberspace support groups may be more serious than those outlined by Reid. King (1996) reports a research study (Finn and Lavitt, 1994) which investigated a nationally accessible sexual abuse survivors support group. The published research report, (whilst valuable for scholars), revealed the identity of members and became a ‘potential nightmare’ for them for years to come as researchers continued to access this report. According to King, Finn down-loaded, analysed and published data without first gaining informed consent, even though ‘Finn reported the existence of a note from the moderator of the group saying that interested professionals who were not sexual abuse survivors were discouraged from joining this group’. King notes Finn justified his action by stating that ‘messages posted on a BBS (bulletin board system) are public information.’
There is a strong temptation for researchers to become ‘lurkers’ in self-help groups, as attested by the venerable researcher and author, Denzin (1999), who confesses that, in his own cyber-research, he has never identified himself to the group ‘nor … obtain(ed) permission to quote from postings, thereby violating many of Schrum’s (1995) ethical injunctions for electronic research’.

**Subtle but significant differences in on-line research**

Schrum (1995) contends that the issue of how private data can be differentiated from public data, when all data exist in the same transparent electronic medium, is the most serious and disputable ethical problem to be resolved both by ethics panels who approve and monitor cyber-research and by the ethical judgement of the individual researcher. While current guidelines for research involving human subjects prohibit the publication of personal and potentially damaging information, the blurred distinctions between the private and the public in cyberspace represent a loophole for bypassing strict adherence to the process of obtaining informed consent, if the individual researcher so chooses.

**Publicly-private**

On-line communication is a unique form of interaction which qualifies participants as a ‘special population’ (King, 1996), for the intertwining of electronic medium and social environment creates special ethical problems for researchers, who must understand and respect that apparently public interactions are perceived by participants as private, and act accordingly (Schrum, 1995).

In on-line fieldwork, researchers can have largely unprecedented access to people’s conversations and stories. Studies have documented the tendency of people to become more ‘open’ when communicating on-line than they are in person (Reid, 1996; Childress and Asamen, 1998; Witmer, 1998). Under a false or exaggerated expectation of privacy, participants may reveal more than they would in face-to-face conversations, and researchers must take account of the risks to the individual posed by this increased lack of inhibitions and not take advantage of human participants who are behaving differently in a unique context which they might define as private, but which the researcher, for the benefits it provides, might define as public. But, as Waskul and Douglass (1996) point out, ‘researchers do not have the right to redefine the context of the research situation to meet their own vested interests and aims’. Schrum (1995) similarly cautions against the liberties taken by some researchers, for ‘although it is possible to join a public discussion surreptitiously for research purposes, it is no more appropriate than taping a conversation without permission’.

**Anonymity**

Even the anonymity of on-line interaction is markedly different from the anonymity required by current standards of ethical research, and the faceless, voiceless nature of this interaction may lead to the objectification of subjects and might impair a researcher’s judgement. To avoid such lapses, electronic ethnographers must remain close to the subjective participant interactions, to counter-balance their easily objectified textual representations (Waskul and Douglass, 1996).
In on-line communities, anonymity serves many purposes for which members believe its preservation is important (Waskul and Douglass, 1996; Witmer, 1998). Merely soliciting participation through informed consent may lead to the feeling that anonymity is threatened, and this may damage the interactions which occur, thus detracting from the experience of the individual.

Anonymity is also the means by which flexible and fluid on-line persona are free to emerge, that is, the ‘possible selves’ (Marcus and Nurius, 1986) which are so difficult to achieve in the physical world. These ‘possible selves’, free of ‘real world’ inhibitions, depend for their construction and maintenance on the contextual and interactive elements of their on-line environments (Turkle, 1995; Witmer, 1998).

Thus, the Internet researcher must be committed to protect not only the anonymity of the individual, but the electronic context itself, and like any other physical research scenario, all identifying characteristics of person and place, including textual statements which might reveal the on-line location should be removed from the research in the course of its data collection and subsequent reporting (Schrum, 1995).

As Waskul and Douglass (1996) point out, anonymity has a further impact on on-line research in respect of the validity and reliability of data, for amongst the widespread geographical and diverse population of the Internet it is easy to conceal and mislead others about one’s true geographical location, age, gender, or race. Such deception may mask also the well-documented existence of a racial, economic and gender divide amongst Internet users, and continue to skew and compound the issue of non-representative sampling, critical to the conduct of certain categories of on-line research.

**Informed consent**

A vital ethical principle of human subjects research is the process of informed consent, which recognises their autonomy by their choosing to become a participant after being fully informed of a study’s parameters and possible benefits or harms, and having the option to withdraw at any time, for whatever reason.

Already complex in its application in the physical world, the process of informed consent is further complicated by the nature of on-line communities (Schrum, 1995; Reid, 1996). Isolating participants is difficult, and membership is fluid. True demographic details, particularly age and intellectual ability, may be hidden under aliases which might lead to the vulnerable (such as children, or persons of diminished mental capacity) being included without the researcher’s knowledge. This constantly changing membership also complicates efforts to conduct debriefings and follow-up research which are necessary in order to assess the long-term benefits or harm to participants.

**Collectivities and sensitive topics**

Schrum (1995) argues the memberships that emerge around sensitive topics should be viewed as closed groups and off-bounds to researchers due to their vulnerability and susceptibility to damage. She provides important guidelines for research with sensitive groups, arguing that most importantly, researchers should negotiate their
entry into these electronic communities through direct discussion with the initiator of the discussion. Participants should be kept informed at all stages of the research of its purposes, benefits, and potential burdens that may result from being studied. Care is mandatory throughout data collection, analysis and reporting of results, to respect the concealed identities of participants, unless explicit permission to use and thereby reveal such information is given.

**Little-understood technical aspects of on-line research**

Lack of understanding by participants (and often the researcher) of the technical and storage capabilities of on-line data may increase the risk of exposure of the participant’s identity and their personal information (Witmer, 1998). For example, e-mail conversations can be archived without the participants’ knowledge and permission, and data from on-line groups are readily accessible for years after the messages were posted. Realisation of the electronic storage of personal information may occur only after the event, when it is too late to withdraw from the project and after personal data has been given, recorded and archived (Schrum, 1995).

**Justice**

Application of the principle of justice bears directly on the recruitment of participants, who should be selected for reasons directly related to the problem being studied instead of their easy availability, compromised position, or potential for manipulation (Commonwealth of Australia, 1999). Applying this principle to Internet research requires identifying the benefits and risks to participants, and dedicated scholarly examination is needed to assess these (Reid, 1996).

**Conclusion: ‘Bottom-up’ Ethical Wisdom**

Waskul and Douglass (1996) point out that ethical codes are not safe havens to hide from the responsibility of making sound ethical choices. Allen (1996), similarly, argues against the reliance on ethical guidelines, which may inhibit the development of a bottom-up ‘ethical wisdom’ built upon concrete experience rather than abstract rules (Bakhtin, 1993). Allen argues that ethical behaviour in researching Internet communities, like that required of the researcher in the physical world, should be based on ‘situated, dialogic agreements’ developed between the researcher and the participants of a research study, which involves an electronic version of the process of gaining informed consent, as applies to other research.

More so than in ‘real’ world research projects, the diversity of Internet research sites, the researcher’s goals, the anonymity of participants, and the social/technical intertwining of human interaction in on-line communities, demands high standards of the ethical judgement and wisdom of the individual researcher, which is underpinned by the researcher’s own knowledge of the fragility of the privacy of participants in cyberspace investigations. The process of gaining informed consent, which is a necessary pre-cursor to the research commencing, must confirm the participant’s understanding of both the technological nature of the storage of personal information (with its potential to endanger the privacy of the individual), and the safeguards undertaken by the researcher to protect individual anonymity.

Allen (1996) suggests that researchers should be required to report on the conditions which have grounded their ethical choices, as well as the consequences for the
participants of these choices. These reflections (if published) would provide a useful tool for building an ethical understanding in the scholarly and wider community of the special need for protecting the electronic participant in cyber-research.

References


The Effectiveness of the Co-Regulatory Scheme for Internet Content Regulation

Geoff Sandy,
School of Information Systems, Victoria University,
Melbourne, Australia.

Email: Geoff.Sandy@vu.edu.au

Abstract

The operational effectiveness of the Co-Regulatory Scheme for Internet Content Regulation is discussed in terms of its specific objectives. It identifies the main arguments about its likely effectiveness of those who supported or opposed the relevant legislation at its preparation and passing in the parliament. It then examines the claims made about its operational effectiveness since that time.

Keywords: Internet and regulation.

Introduction

On 1 January 2000, the Australian Federal Government’s Broadcasting Services Amendment (Online Services) Bill 1999 was proclaimed. The purpose of the Bill is to establish a framework for the regulation of the content of online services. This is referred to as the Co-Regulatory Scheme for Internet Content Regulation (hereafter the Scheme). Specifically, the Bill seeks to:

1. provide a means of addressing complaints about certain internet content
2. restrict access to certain internet content that is likely to cause offence to a reasonable adult
3. protect children from exposure to internet content that is unsuitable for them

In a relatively open society like Australia all political parties claim to support the principle that adults should be able to read, hear and see what they want. None would consider this as an absolute right to “freedom of expression”. It is how this is interpreted that gives rise to different views about the justifiable degree of government censorship. Equally all would wish to protect children from unsuitable material but differ as to how this is to be defined, and as to the proper role of the Government in this regard. The Bill was prepared by the ruling conservative coalition but was opposed in part or whole by the opposition parties.

This paper discusses the effectiveness of the Scheme in terms of its specific objectives after two and half years of operation. It identifies the main arguments about its likely effectiveness of those who supported or opposed the Bill at the time of its preparation and passing through the parliament. It then examines the claims made about its operational effectiveness since that time.
The primary source documents used for this research are:

1. The Official Committee Hansard of the hearings from the submitters on the Broadcasting Services Amendment (Online Services) Bill 1999 by the Senate Select Committee on Information Technologies
2. Senate Hansard of the second reading of the Bill
3. House Hansard of the second reading of the Bill
4. The Broadcasting Services Amendment (Online Services) Bill 1999
5. Department of Communications, Information Technology and the Arts, Bi-Annual Reports of the Scheme
6. Official Media Releases

Throughout the paper reference is made to (1) above as the “hearings”, (2) and (3) as the “debates” and (4) as the Bill. The abbreviated in-text citation used throughout for (1) is “SSC” for Senate Select Committee, (2) is “SH” for Senate Hansard and (3) is “HH” for House Hansard. Full details are provided in the references section. Acknowledgement is made of the reliance on the work of Electronic Frontiers Australia (EFA). EFA is the premier civil liberties group regarding the internet in Australia. Its views are representative of those opposed to the Bill and those who claim the Scheme is ineffective.

Providing a means of Addressing Complaints

A specific objective of the Bill is to provide a means of addressing complaints by Australian residents or a body corporate that carries on activities in Australia about certain internet content. On receiving a complaint about internet material the ABA can require an Internet Service Provider (ISP) to take down X rated or refused classification material (RC) hosted onshore, and to take all reasonable steps to prevent access to X rated or RC material hosted offshore. In respect to restricted (R) classified onshore content the ABA must be satisfied that restricted access arrangements are in place. No proposal is made in respect to offshore R classified material. The Bill expressly specifies time frames for the take down process and penalties for non compliance.

Australia uses a classification system to determine the degree of censorship that is to be applied to a variety of offline media that includes films, videotapes, publications and video games. The Classification Board of the Office of Film and Literature Classification (OLFC) undertake the classification. The State and Territory Governments also use this although some adopt a more rigorous interpretation. Classification decisions apply criteria that are part of the National Classification Code. The most important “test” that determines a particular classification is the concept of a “reasonable adult”. Such a person is defined officially as “possessing common sense and an open mind, and able to balance opinion with generally accepted community standards” (OLFC 1999b).

The Bill envisaged the establishment of a community advisory body on internet content now known as NetAlert. In a media release Minister Alston (1999) said that “NetAlert will be responsible for researching new access management technologies and running national awareness campaigns to promote a safer internet for young people”. He saw NetAlert as “an additional measure that will play an important role
by empowering parents to take control of the internet so that they can feel confident about their children going online”.

The supporters of the Bill claimed the legislation was in response to a major concern expressed by the community about internet pornography (SH 5218; HH 6907). During the debates the coalition claimed the Bill had attracted little or no criticism from the public (SH 5218) and Minister Alston asserted that internet pornography is a major social problem for Australia. Indeed, some coalition members believe the internet is awash with pornography with the claim that it constitutes 60% of its content (SSC49; 73). Internet industry representatives at the hearings reacted with incredulity to this claim (SSC 49; 73).

No comprehensive study on community attitudes to internet pornography has been conducted in Australia. Both supporters and opponents of the Bill provide anecdotal evidence to support their case (SH 5210; 5212). What empirical evidence exists suggests that internet pornography is not a major concern (SSC 260ff; 297-299). However, few Australian would support child pornography and Minister Alston (2001), in a media report cites a recent survey by AustraliaSCAN that found 97% of Australians are opposed to child pornography. It can be argued that the establishment of a formal mechanism to process complaints and publicizing that fact can act as a self-fulfilling prophecy. In other words the very act of establishing a mechanism to deal with a perceived social concern may create the social concern. Sensational press stories about internet porn can also act to “manufacture” concern when it is not strong.

**Restrict Access by Adults to Offensive Material**

The classic libertarian position is to treat freedom of speech as indispensable to the open society. If the government wishes to censor some type of speech, like pornography, then the onus of proof of demonstrable harm rests with the government. State intervention to censor pornography without empirically proven evidence of social harm is an illegitimate exercise of state power in an open society. During the hearings and the debates offensive and unsuitable material was almost invariable equated with pornography. Surprisingly little was said about equating harm of the “reasonable adult” with feelings of being offended by an image and/or text. This is central to the governments system of censorship of any media. Vital to a view on pornographic harm is the meaning and power of the pornographic image (Sandy 2001). One view is that the pornographic image is a master text to practices it portrays. It does represent real (bad) attitudes and desires, and, it teaches the consumer these attitudes, and to expect to recreate these practices in reality. As indicated previously there is little empirical support for this view. Many supporters of the Bill accepted this view (SSC 108; SH 5212-5213).

The opposing view is that the pornographic image is a signifying system and a fantasy scenario. What is portrayed is not the object of desire but a scenario in which certain wishes are presented. This may involve scenarios that are illegal as acts. Fantasy is clearly a separate realm from reality and cannot be taken at face value. Opponents of the Bill tended to make this distinction an claimed the Bill would violate the freedom
of an adults (SH 5199;5207;5213). The representative of the Australian Computer Society, for instance, spoke for many when he argued that the internet should remain an adult medium and should not be transformed into a media suitable only for children (SSC 72). This he claimed would be the effect of the legislation.

Supporters of the Bill asserted it did not suppress free speech (SCC150; HH 6907; SH 5219). Further, the coalition countered that the internet warranted no special treatment in regards to government regulation compared to the other media (SH 5219; HH 6970). What is censored offline is now to be censored online. However, this begs the question about whether censorship of other media is justified.

Most research studies on pornographic harm are for media other than the internet. Australia lacks empirical research in this area. As is common for any contentious area each group holding different views claim the research findings support their particular view. Pornographic harm is no exception. Sandy (2001) summarized these studies and they suggest there is no causative link between sexually explicit material and acts of violence (non consensual) or in a change of male attitudes (for the worse) towards women. This is whether the sexually explicit image is accompanied by violence or not. It appears that there is little empirical support to justify censorship of pornography in an open society on the grounds of it being harmful to adults. If this is accepted then this applies to all media and not just the internet.

In regard to minors and pornographic harm there are no reported studies for obvious ethical reasons. In the case of images of pedophilia or images of incest with minors it is widely agreed that these be illegal because it is assumed that production of such images involve non-consensual acts. Recently, the Supreme Court of the United States ruled that legislation that made morphed child pornography images illegal was contrary to the First Amendment.

EFA claim that the Scheme is one component of a wider strategy by the coalition and other conservative forces to curtail adult freedoms. The “evidence” cited includes:

1. tighter regulation that goes beyond pornography to adult themes, especially in regard to films (EFA 1999)
2. failure to approve a change from X rated videos to Non Violent Erotica (EFA 2000c)
3. more restrictive treatment of computer games (OLFC 1999a)
4. standardisation (more restrictive) of classification criteria used by the OLFC (EFA 2000b)
5. proposed “excessive and overboard” Cybercrime Bill 2001 (EFA 2001a)
6. “tougher” Telecommunications (Interception) Legislation Amendment (EFA 2001b)
7. proposed “profoundly flawed” New South Wales Internet Censorship Bill 2001 (EFA 2002a)
8. proposed “profoundly flawed” South Australian Net Censorship Bill 2000-2001 (2002b)

All of these examples pre-date September 11. Libertarians are concerned that we now operate in a climate that is more conducive to legislating away adult freedoms.
Protection of Children

The issue of protection of children from unsuitable material was a dominant one during the hearings and debates. It remains the key issue in discussions about the operational effectiveness of the Scheme. All parties agree that both parents (including teachers, librarians etc) and the government have a role in protection of children from unsuitable Internet material. The main disagreement concerns the degree of freedom left to the parent to determine what material the child consumes.

Supporters of the Bill argued that the Government must be pro-active in doing all it could to assist parents and guardians in undertaking their parental responsibility. The coalition members argued that the Scheme would support parents who lack the technical knowledge necessary to properly supervise their children’s access to the Internet (SSC 51; SH 5219; HH 7977). Much was made by them of portraying children as more technically competent than their parents, and because of this, are able to deceive their parents about their Internet use. Implicit in the arguments of some supporters of the Bill was that it would counter irresponsible parents who did not properly supervise their children’s Internet access (SSC 51; 157-158; SH 5219; 5212). The Bill was considered necessary to protect children from their own (irresponsible) parents.

Coalition members at the hearings adopted a similar view towards library staff in regards to supervision of Internet access by children in libraries. They suggested that library staff are too busy to be monitor breaches of policy, and given the tenor of questioning an implicit suggestion that the library policy on this matter borders on the irresponsible (SSC 192ff; 103).

Originally the Government believed that unsuitable material could be successfully blocked at the ISP or “backbone” provider level. Those opposed to the Bill argued that the best place to block content is at the receiver and not the ISP or backbone provider (SSC 151ff; 243ff). The findings of a report by the Commonwealth Scientific and Industrial Research Organisation (CSIRO 1999) were given prominence in the hearings and debates. It was treated as authoritative by both sides. The report considered blocking access at the ISP or backbone provider level to be largely ineffective. Instead it recommended the use of filtering software by Internet users. It evaluated the effectiveness of filter products and commented on their deficiencies.

The coalition acknowledged the deficiencies of the filter products but looked forward to a future where technology had developed to such a state that it would make the Bill more enforceable (HH 7978). Until then the coalition responded by stating “the fact that some aspects of the bill are in the opinion of some in the industry, unlikely to succeed is not argument enough, for the government to ignore this issue and to allow the Internet to go unchecked as a conduit to the world’s unsavory material for our children” (HH 7978). More recently the CSIRO (2001) has evaluated the effectiveness of 14 Internet filtering software on behalf of the ABA. It found that they vary considerably in their effectiveness in blocking targeted material.
A common argument made by those opposed to the Bill was that not only is the blocking software ineffective in protecting minors but the charge that the government is deceiving parents into believing the technology is trustworthy (HH 7970ff; SSC 257-258; 104). Thus, parents are “lulled into a false sense of security” (SSC 245) and therefore “the Bill could do more harm than good” (SSC 63). Further, it was argued that the government by putting its faith in software that does not work results in a lost opportunity to educate and empower parents to take responsibility for supervision of the internet by their children (SSC 6914).

The strongest claim about the likely ineffectiveness of the Scheme was by industry spokespersons at the hearings (SSC 63ff; 127ff) and of others in the debates (HH 7970; SH 5136). They argued that the legislation will not work because over 90 per cent of the content is hosted offshore. The supporters of the Bill were also reminded of the ease with which domestic sites could move offshore to escape enforcement (HH 6913).

Some opposition members (SH 5199; 5210) and submitters to the hearings (SSC 48-49; 70) pointed out that the Bill is not needed because the existing laws, especially the Crimes Act, are adequate to deal with illegal activity online. An industry spokesman at the hearings succinctly put it “as far as we know there are no illegal activities that become less illegal on the internet” (SSC 209). However, the hearings were told that some uncertainty exists as to whether the Crimes Act does cover the internet (SCC 123). The coalition indicated it would legislate to rid the Act of any uncertainty (HH 6907).

Opponents of the Bill stressed during the hearings and debates (SSC 244; 262ff; SH 5198ff) that a society, like Australia, is composed of many communities of widely differing standards in relation to sexuality, gender relations and sexual expression. One of Australia’s greatest assets is a social structure that is highly pluralistic. In reality, the “test” of the "reasonable adult" results in the majoritarian norm being forced on all communities. In an open society like Australia, speech that is deemed illegal or restricted should depend on “proving” its demonstrable harm. In the absence of this mere offensiveness to a group is no justification for censorship by the state.

**Operational Effectiveness of the Co-Regulatory Scheme**

In an attempt to gather evidence of the Scheme’s ineffectiveness EFA in February 2000 lodged a FOI with the ABA seeking material banned and not banned under the Scheme. It was seeking evidence to “prove our point that the system put in place will not work and cannot ever work. The whole system’s basic concept is flawed because most content on the net is hosted outside Australia so there is nothing the Government can do about it”(EFA 2000a). Six months later some documents were released by the ABA. EFA accused the ABA of a “net cover-up” (Jackson 2000). After examination of the released documents EFA (2000a) made the following claims about the operational effectiveness of the Scheme:

1. The blacked out URLs were not only of banned pages but for papers not banned.
2. Discrepancies exist between the information released and the ABA’s first quarter report issued in April (ABA 2000) and Minister Alston’s first bi-
annual report on the Scheme tabled in September (Commonwealth of Australia 2000).
3. the ABA had gone beyond its legislature remit and made a value judgment as to what may harm if the URLs for certain non-prohibited content are released.
4. the ABA has acted on and prohibited content as a result of complaints received from non-Australian residents.

In media releases Minister Alston (2001a; 2000) claims the internet is safer for all Australians because of the work of the ABA of continual removal of illegal and highly offensive material on the internet particularly child pornography sites. He refers to the second and third bi-annual reports on the Scheme (Commonwealth of Australia 2001; 2002). Referring to the second bi-annual report he indicates that the ABA completed 221 investigations of which 139 resulted in a location of prohibited or potentially prohibited content. He states “this represents a 49 per cent increase in the number of completed investigations which located such material in the first six-month period and demonstrates the Scheme’s continued effectiveness in addressing public concerns regarding the nature and accessibility of some Internet content”. He believes “Australian families will welcome the continued removal by the Online Content Regulatory Scheme of illegal and highly offensive material on the Internet, particularly child pornography sites”. He also discusses the work of Net Alert in assisting industry to reach full compliance through the development of an information manual and a series of national industry compliance seminars targeting smaller ISPs. In addition he states that NetAlert and the ABA are working on research and community education initiatives. Specifically, NetAlert’ advisory services, toll-free national help line, information kit and website are mentioned. Similar reference is made in the third bi-annual report.

EFA (2001c) and others claim that the Scheme has failed to achieve its objectives. First, the ABA has gone out of its way to portray the reported figures in a way that overstates the apparent effectiveness of the Scheme. The ABA’s Internet Content Complaint Form clearly states you can only complain about one item of internet content in each complaint form. However, the ABA in the second bi-annual report indicates 67 “items” of prohibited content from 6 Australian sites. In contrast 136 items of prohibited content were reported in respect of the 133 overseas sites. The third bi-annual report indicates that the ABA issued 8 take-down notices to Australian hosts covering 37 items of prohibited content. EFA believes the ABA is ramping up the “item count” in order to make the figures look respectable in relation to Australian content.

Second, of the 67 items of prohibited content 45 items (child pornography) from 6 Australian sites were referred to the State/ Territory Police. Similarly, of the 37 items 23 that are child pornography were also referred. It would appear no successful prosecutions have been undertaken. EFA claim most of these complaints relate to newsgroups.

Third, Minister Alston is criticized for “misleading political rhetoric” that grossly overstates the impact of the Scheme. This lulls Australian parents into a false sense of security. The claims made by him play on the emotive impact of the child pornography bogieman, without any supporting information about prosecutions of Australians for publishing such material.
Fourth, EFA estimates that the total cost of the Scheme for the first 12 months of operation is $2.5m. and suggests the benefits are not cost effective. It suggests the impact in Australia has been the cancellation of a number of newsgroups and a few adult Australian web sites forced offshore (Forbes 1999). Further, it is claimed that NetAlert’s activities are equally questionable in terms of outcome.

Fifth, EFA suggests that by encouraging Australian citizens to report child abuse material to the ABA, the process places complainants at risk of committing a criminal offence. The mere awareness of the existence of such material implies that it has been downloaded into the complainant’s computer. It is noted that there is nothing in the Bill that grants immunity from liability for persons reporting illegal content.

Sixth, it is claimed that the ABA fails to disclose what content has been removed and why. This is different from the treatment of offline content (Taggart 2002). David Flint, Chairman of the ABA counters by stating that the internet is different from the offline media and believes that making child pornography URLs public will jeopardize the policing and legal processes (Taggart 2002).

Seventh, Minister Alston (2001b) claims that the success of the Scheme will lead to an uptake of the new technology by families and this in turn will drive the growth of the new economy in Australia. However, McAuliffe (2001) points out that the latest Bureau of Statistics figures show the number on internet subscribers in Australia rose by 3.9 million at the end of the December quarter but there were 7,000 fewer household internet accounts and decrease in 307,000 free internet accounts. The Bureau believes the decline is due to industry restructuring and ISPs going out of business.

**Conclusion**

The key test regarding the operational effectiveness of the Co-Regulatory Scheme is whether it has lead to significantly greater protection of children from unsuitable internet content. Supporters of the Scheme claim that this is the case and is evidenced by:

1. the issue of take-down notices and referrals of illegal material (child pornography) to the federal police of sites hosted overseas and to the state/territory police of sites hosted in Australia.
2. the work of NetAlert on research for example the technical evaluation of filters by the CSIRO
3. the work of NetAlert community education initiatives for example promotion of the Australian Families Guide to the Internet web site and presentations at various conferences.

Opponents of the Scheme claim the Scheme is ineffective principally because overwhelmingly unsuitable content is hosted overseas and all the Government can do if it is illegal is to refer it to the federal police. Australian sites referred to the state/territory police are few and there is no evidence of any successful prosecutions in relation to these. Critics of the Scheme remain unconvinced the Scheme was necessary as such material was and is covered by the states/territory’s Crime Acts.
Further they assert that parents may be lulled into a false sense of security believing the Scheme to be effective in protecting children when it is not.

At this stage the weight of evidence suggests the Scheme has not afforded children significantly greater protection against unsuitable internet content.

References

Alston R (2001b) Growing Internet and Computer Use Media Release, 8 May.
Alston R (1999) Internet Content Advisory Scheme Announced, Media Release, 26 November.
Commonwealth of Australia (2001) Sixth Month Report on Co Regulatory Scheme for Internet Content Regulation July to December 2000 Department of Communications, Information Technology and the Arts, April.


McAuliffe M (2001) *Oz Home Internet Subscribers Drop* ZDNet Australia 1 May.

Office of Film and Literature Classification (1999a) *Guidelines for the Classification of Computer Games: Amendment No. 1.*

Office of Film and Literature Classification (1999b) *Guidelines for the Classification of Films and Videotapes: Amendment No. 2.*


Accessible E-Commerce: Crossing the digital generation gap

Helen Scott¹, Oliver K. Burmeister², and Steve Roberts³

¹Information Manager
Council on the Ageing (Australia)
E-mail: hscott@cota.org.au

²Swinburne Computer-Human Interaction Laboratory
School of Information Technology
Swinburne University of Technology, Australia
E-mail: oburmeister@it.swin.edu.au

³Senior Technology Specialist - Usability
National Australia Bank, Australia
E-mail: Steve_Roberts@national.com.au

Abstract

Several recent initiatives have increased the accessibility of e-banking for older people in Australia. Government and the private and community sectors have built significant bridges to cross the digital generation gap. Yet there are policy deficiencies and a lack of partnering with the community to create interconnectedness, particularly in terms of resourcing. This is particularly evident in macro level issues which need to be better coordinated across tiers of government. Community and consumer groups need to be better resourced to enable people to take advantage of e-services. There is an ongoing need to be socially responsive and responsible toward senior citizens through better supporting their values of respect, dignity, independence and social-interconnectedness.

Keywords: Ageing, digital divide, e-banking, e-commerce.

Introduction

Significant progress has been achieved in crossing the digital generation gap that has kept large numbers of the Australian community from accessing e-commerce applications often taken for granted by the majority. Yet an inclusive approach that takes account of and gives dignity to senior citizens is only in its emerging stages. This paper examines the progress made, along with shortfalls in both government and the private sector that still need to be addressed. Discussion of e-commerce is limited to e-banking.

On April 15th this year the Australian Bankers’ Association (ABA) released new voluntary Industry Standards aimed at improving the accessibility of electronic banking. Launching them, David Murray, Chairman of the ABA, said: “The Industry Standards are important steps in helping overcome the digital divide and will assist individual banks develop or enhance their electronic banking services for older Australians and people with disabilities.” (ABA 2002a, p 1)
These new standards arose from identification of an emerging digital divide between those people who could utilise new technologies to improve their lives and those who could not, and were developed by working groups representing all sectors. The standards are designed “to begin the process of eliminating the digital divide by dismantling e-commerce access barriers” (ABA, 2002a, p 1). According to the (Commonwealth) Disability Discrimination Act (DDA) all services and facilities provided by businesses, be they government or in the private sector, are to be accessible to people with disabilities.

Sev Ozdowski, Disability Discrimination Commissioner, addressing the new ABA standards said “Many people with disabilities will for the first time be able to independently and privately conduct their financial transactions electronically … This is something most of us take for granted. Now people with disabilities can enjoy the same right.” (ABA, 2002b)

Maryanne Diamond, Blind Citizens Australia Executive Officer, similarly agreed that these new standards for electronic banking would improve the independence and dignity for older people and people with disabilities. [Note: throughout this paper older people are distinguished from people with disabilities despite the fact that approximately 50% of the Australian population over 60 years have a disability (ABA, 2002a). This is because most older people view their disabilities as the result of ageing, they do not consider themselves to be people with disabilities. Then too the reader should be aware that there are people with disabilities who are ageing and classify themselves both as ageing and as people with disabilities. A general guideline for talking with seniors is to use terms such as ‘age-friendly’ as opposed to ‘disability-friendly’ technological products.] Maryanne Diamond, who is blind herself, went on to state:

“Until now, I have been forced to rely on over the counter, face to face banking services, or to reveal personal financial information, including my PIN, to third parties. This was clearly unsafe, but equally important, it was demeaning. I’m blind, not incompetent … Ready, independent access to services like ATMs makes banking faster, safer and more efficient. It also helps me to keep my self respect”. (ABA, 2002c)

Older people are widely recognised as one of the population groups on the wrong side of the digital divide. When talking about older people it is important to stress their diversity, not just statistics about growing numbers due to population ageing (below).

**The digital generation gap**

Koehler (2001) defines the digital divide as two distinct but related social and ethical issues. These two issues are:

- Information and digital literacy equity within countries; and,
- Information and digital literacy equity between countries.

Both issues relate to the gap between those who have access to information and who are digitally literate and those without such access and literacy. This paper is concerned about the first issue only, and is further restricted to the “gap” in terms of it
being a generational gap – a gap that excludes older generations from participating in the benefits, perceived and actual, of the information revolution known as e-commerce.

Information literacy and use of the basic technology tools is a pre-requisite skill for participation in Australia's economy and a matter for public policy. The reality is that people without computer literacy, or at least literacy in technology, are already becoming second class citizens. They are further disadvantaged by their inability to use computers to search for a job, to broaden their education, to socialise, to conduct their basic banking needs, access information or even participate as volunteers in community organisations. Brink (1997) speaks of a ‘Digital Dividend’ defined as “the benefit from use of digital technology over and above other technologies, which may be economic or non-material in terms of time, effort, satisfaction and social capital”. That is, aside from providing people with age-related disabilities access to e-commerce technologies, there is a wider dimension of social responsibility – this wider dimension is picked up on in the discussion of values below.

The size of the market

Senior surfers are one of the fastest growing groups on the World Wide Web (Scott, 1999) - Australian Bureau of Statistics (ABS) figures show a 220% increase between May 1998 to May 2000 for persons aged 55 or older (ABS, 2001b). Despite this, the current generation of older Australians has a relatively low rate of use of electronic technologies and even lower rates of e-shopping and banking. Recent data shows that the “number of registered online banking users in Australia almost doubled in the past year to reach 5.23 million at the end of March 2002, up from 2.77 million in 2001. Users aged 50-plus recorded the biggest growth rate of 113 percent to reach 775,000 for the 12-month period.” (Gal, 2002; note, these results were qualified by the comment that the proportion of active rather than registered users is quite small.)

The proportion of people aged 65 and over in Australia in 2001 was 12.6%, 2.38 million (ABS, 2002). This has been forecast to increase to 17.2% in 2025, and a quarter (24-26%, 6-6.3 million) by 2051, part of a common trend in the developed world where fertility and mortality are declining. The overwhelming majority live independently at home, either with a partner only (46%), family (17%) or alone (28%). (ABS, 1999)

Considering the needs of the ageing also has elements of self-interest. Vanderheiden (1994) pointing to US studies states that by age 55, 25% of the population will experience functional limitations, 50% by age 65 and 70% by the time we reach 70 years of age (should we be so fortunate). Australian data shows that 54% of over 65 year olds in 1998 had a disability, rising to 84% of people over 85. (ABS, 1998). So aside from considering the needs of the ageing, as though ‘they’ are some other group, we should give thought to our own ageing and to our desires for adequate access to technology in our own old age.
Socio-economic considerations

Designing for access to e-commerce needs to take into account that this requires use of low-cost technologies, readily available to people in the lower socio-economic bands of society – which is where most people with disabilities are located according to a study by the Human Rights and Equal Opportunity Commission (HREOC, 1999). Income inequalities abound - some groups are well-off (the over 65's head up households owning almost half the deposits in the nation's financial institutions), but in fact poverty is the reality for many - 48% of retirees are among the poorest 30% of Australians (ASFA, 2001). Most older Australians are on a low income - 75% of the eligible population receive government pensions as their principal source of income (ABS, 2001a).

Funding programs do not necessarily address these inequities. False assumptions are that funding generalist programs picks up everyone, and that community projects do not need ongoing funding after 1-3 years, particularly in rural areas relying heavily on volunteers. Training programs for example have been mostly in metropolitan areas and taken up by people with higher socio-economic status and education levels. Groups with multiple disadvantages, such as older people in rural areas with low income, limited education, low literacy, English as a second language, and indigenous groups miss out unless targeted. The needs of small communities are generally unmet, Tasmania being the exception. The pervasive nature of stereotypes about age result in age discrimination in employment and training for older workers.

In Australia the debate over the digital divide has taken a regional focus due to differences in metropolitan and regional rates of access. However, recent Australian research (NATSEM, 2000) supports overseas findings showing that socio-demographic factors are more important in influencing access to new technology, not regional ones. The most important drivers of Internet access are educational qualification, income, and age, not geography. These results suggest that supply-side policy solutions which have dominated so far will not be sufficient to overcome the digital divide. The Coalition Government's emphasis on private sector competition policy for infrastructure and increased data speeds, and on Networking the Nation funding for rural areas is not an overall or successful policy for addressing the digital divide, and specifically does not address use, access or building online communities for disadvantaged groups or older people. Very few Networking the Nation programs went to older people judging by the NOIE (2000) directory.

A related caution about training is that where age related functional disabilities require the use of adaptive technology, it is highly unlikely that the training facilities will have the appropriate technology. Currently the way training programs are funded, government assistance for adaptive technology is only provided for the individual enrolling in the course. Given the large expense associated with providing multiple, alternate adaptive technologies, few training organisations have this available. This further limits the ability of seniors with disabilities from being able to cross the digital generation gap.

One further consideration in regards to seniors and some people with special needs is that they can take significantly longer than younger people to perform tasks, which has a cost impact for them on ISP, particularly broadband, charges. As with utilities
and councils there should be a reduced ISP charge for pensioners or people with special needs.

**E-banking technologies**

There are four main areas of e-banking addressed by the new ABA standards. As will be seen in the discussion that follows, the standards have so far only partly addressed the concerns of these citizens. Adoption of the new standards is voluntary, and consumers are sceptical about relying on good will, questioning whether major financial institutions which function quite independently for competitive reasons will be committed to adopting them and addressing any complaints or breaches that arise. Another reason for the financial institutions working independently on this topic is driven by restrictions placed on them by various legislations, such as the Trade Practices Act. Governments need to legislate to provide exemption where combined work would benefit the community.

*Automated Teller Machines (ATMs)*

One recent initiative to solve the needs of seniors and others with visual disabilities has been the introduction of voice-enabled ATMs (NAB, 2002), through an initiative jointly supported by the NAB’s ATM supplier (Diebold) and Blind Citizens Australia (BCA). The first of these was installed at the Royal Victorian Institute for the Blind (RVIB), in Prahran, Victoria. NAB says that all their new ATMs from January 2003 onwards will be voice-enabled. ATM users cite convenience, ease of use and time saving benefits. The major concern of non-users is safety (Owens, 2001, p 46); such as fear of mugging especially if frail. “I'm concerned about security, I don’t go to ATMs in the street. I use ones that are under surveillance” (Owens, 2001, p 47).

A drawback in using an ATM or EFTPOS is that it can be a very public display of competence in a queue!

A problem for all users, not only those older or disabled, is the difference in design, user instruction and formatting at the various outlets.

*Electronic Funds Transfer at the Point of Sale (EFTPOS)*

In most cases where bank staff have performed field observations of customer use of this technology, the ‘checkout’ operator pressed most of the keys except for keying PIN number or pressing the Account selection key and then the OK key. That is, one advantage of the EFTPOS terminal was that there was a knowledgeable person there to assist.

Trainings with bank staff have led to observations that this is a technology in which support for the ageing is less likely to be an issue. This advantage of the operation of EFTPOS terminals is not just restricted to older people. It may be that the operators find it quicker for themselves to press the buttons. A considerable number of users are still confused when asked is ‘that Credit, Savings or Cheque?’ Many people have to stop and think which account they want the goods charged against. The terminology used could be confusing especially if they have “nicknames” for their accounts (one is their ‘cheque account’, one is ‘normal’, one is ‘savings’ and another is for the ‘car’).
An additional advantage for seniors is that of a perception of safety, as seen in this quote by Owens (2001, p 49) “I prefer to use EFTPOS to ATMs, not open and exposed to the public”.

*Automated Telephone Banking [also known as Interactive Voice Response (IVR)]*

Council on the Ageing (COTA, 2001) relates a respondent saying: “I recall my father in law just a month ago having a very deep conversation with ‘a lovely lady’ for several minutes only to be confused when he was abruptly cut off – when I re-dialled the number I found he had been talking to a machine!”

A good feature of the new standard is that it allows for the option to speak to an operator, and automatically transfer to an operator when the customer doesn't respond, without financial penalty.

*Internet Banking*

To keep electronic customers, systems must be excellent - software or hardware glitches are not acceptable, particularly now there are fees for using online services. Pet hates for any consumers are crashing servers, sites that rely on high speed connections and up-to-date computers (older people often have low performing "hand-me-downs") and site updates that make original set-ups invalid. Such difficulties would be largely overcome if website designers were fully cognisant of accessibility guidelines.

Internet banking facilities also need to have the ability to be customized by the user. For example, specific names attributed to different accounts by the user - "Sam's savings account", "Joint Mortgage account", "Mary's credit card account". Seniors find such name attributions helpful as this reduces the load on memory. It allows easy recognition of accounts by not having to associate a large string of numbers to an account type. (NAB allows customers to allocate a “nickname” to their accounts via Internet Banking.)

In summary, the above e-banking technology discussion illustrates that while the universal design principles adopted by the ABA and reflected in the new standards are a significant first step, there are universal design issues that are transgenerational, the implementation of which may be hindered through the independent nature of the standards implementation. Though the discussion is focussed on people with age related functional disabilities, the issues raised here are not issues that only affect a minority who have needs for separate, adaptive programs focusing on age or disability deficits. With each bank taking a voluntary, independent approach, the inter-bank or macro level issues can be overlooked – adopting a colloquialism, the focus is on the trees, not the forest. This is true too in the discussion which follows regarding the government approaches to solving the issues – individual department or tiers of government apply solutions to individual trees, but this is not ‘universal’. A universal principle needs to be applied to the forest, at the macro level, for all the trees to get the benefit.
Motivation and values

How do ‘universal design principles’ come into being? One could see these as transgenerational principles about the best fit (or interaction) between technology and people. But in order to better understand the human side of the equation, one has to consider the motivations and values people have. In that consideration this paper is again restricted to seniors.

West (2002), using data collected from 2000 participants in a Seniors-On-Line project and 337 participants in a Technology Classes for Older People project and by referring to the work of other researchers, identified three main motivational themes, that despite individual differences, appear to be significant in the lives of older people when using technology. These are:

- Remaining independent;
- Being in control of one’s life;
- Connections to family and community.

In attempting to comply with the new ABA standards banks are implementing a number of initiatives. Amongst these is one by the NAB to train staff already dealing with the needs of ageing customers in better helping them with e-banking products. The following are a list of responses by those NAB staff, given when asked to describe what they thought the needs of their aged customers are, that is, based on their experiences with such customers, parents or grand parents.

- Don’t like change – it worked ok before so why change
- They find new technologies confusing
- There is great distrust
- There is fear of losing it all
- They have plenty of time on their hands
- They like to have a talk thus they want people to people interaction
- As they get older and older there is a reliance on family members helping them with technology, finance, etc. Losing this independence.

The observations are similar to the research findings of Hawthorn (2000), who has carried out extensive studies of functional abilities amongst people from 20 to 70 years of age.

A HREOC inquiry into the *Accessibility of Electronic Commerce and New Service and Information Technologies for Older Australians and People with a Disability* (HREOC, 2000), as well as papers by Scott (1999, 2001a, 2001b) show that digital generation barriers include:

- set-up and access costs;
- physical inaccessibility/difficulties in using many electronic services;
- website inaccessibility;
- attitudes such as fear;
- a perceived lack of relevant content;
- safety and security concerns (especially for ATMs and EFTPOS);
- lack of skills and training;
illiteracy.

One might abstract from West’s motivations, the values expressed by seniors to NAB staff, the HREOC study and work by COTA, the following higher order values for seniors when engaging in e-banking activities:

- Independence and deriving a feeling of being in control of one’s life.
- Security (the perception of).
- Freedom of choice.
  COTA has frequently argued that providers of online services – whether this be online bill payment, banking services or downloading publications, must provide alternative methods of access without financial penalty for those unable or unwilling to access them electronically.
- Connectedness to family and community.
- Dignity. In many societies showing dignity or respect to one’s elders is part of the cultural imperative. Yet as seen in the quote from Maryanne Diamond above, when it comes to e-banking we demean some of our citizens.

When incorporating these values into universal design principles, the digital dividends increase significantly. No longer is the emphasis on the micro issues of enabling access to people with one or another type of disability. Nor is a solution by one bank or one government department sufficient. Solutions for the human side of the interaction between seniors and e-banking requires consideration of the motivations and values they have. Engagement with community groups at a level where they perceive real benefits will accrue to them from participation is required - the best way of spreading the word amongst older people is older people themselves. Here is a bridge to the digital generation gap.

A few solutions

Some of the solutions are inherent in the type of language used to describe the digital generation gap and the bridges across it. Terms such as ‘age-friendly’ as opposed to ‘disability-friendly’ technology, ‘learning for life’ as opposed to ‘learning for work’ and (Heath, 2001) ‘connected community’ as opposed to ‘information economy’, encapsulate the values of older people as seen above.

The HREOC (2000) inquiry's report specifically highlighted the difficulties around adaptive equipment, web page inaccessibility, access difficulties for e-banking facilities (ATMs, EFTPOS and IVR) and other automated devices. Its recommendations encompassed the need to complement online/automated services with human ones (as seen in the EFTPOS discussion above, and by COTA's continued representation of older people's desire to retain face to face services), information provision, community access points, education and training, recycling, standards development, universal design and website accessibility. It is to be hoped that users will be involved in design and trialling any new initiatives, as recommended by the standards.

Older people are a growth market for technology products and education, and need to be recognised not as technophobes, but as a vital consumer group who will purchase and access technologies if they are useful to them. Chronological age is less
significant to utilisation of technology than the presence or lack of technological skills, disability, infirmity and dependency. Attitudes to technology are affected by the perceived benefits of using it, positive past experiences, quality of information and instructions about it, training and follow-up, hands-on experience, and the extent to which it meets user needs. (Scott, 1999)

Incentives for compliance or disincentives for failing to comply should be considered as part of the government policy. Current government policy is not an incentive to corporations/businesses as they are taxed for employing people through payroll taxes, superannuation charges, work cover and more. Tax incentives for those who are complying or heavy penalties for those not would encourage action to be taken.

The private sector

The private sector response to the voluntary standards of the ABA has been varied. The NAB are updating their own Disability Action Plan (DDP), expected to be released in September 2002. [There is a register of over 180 DDA action plans online at www.humanrights.gov.au/disability_rights/action_plans/Register/register.html]. They have also introduced training for staff as seen above, which shows an understanding that to properly address the needs of ageing consumers, not only do those consumers need to be trained in the use of e-banking technologies, but bank staff need to become better acquainted with the needs of senior citizens.

COTA in cooperation with the Commonwealth Bank of Australia (CBA) introduced and resourced self-service banking programs to their network of approximately 2000 clubs. Retired CBA staff introduced club members to electronic banking by bringing ATMs and EFTPOS equipment, so that members could practice without the pressure of a public environment. No differentiation was made between CBA customers and customers of other banks. CBA also upgraded staff training, produced a specialist video and produced large print brochures. Since then the CBA has partnered with COTA NSW to establish the Sydney COTA/Commonwealth Bank Online Learning Centre to provide older Australians with access and assistance to online technology.

Further funding, sponsoring and partnerships to develop practical innovative grassroots education and access programs needs to come from the banking and finance industry, and government. Community partners should not be expected to subsidise commercial organisations or government by providing information, expertise and a constituent audience via their networks unless they are properly resourced, like the CBA did in the example above. The many good education programs run by COTAs, the Australian Seniors Computers Clubs Association, Universities of the Third Age (U3A) and similar initiatives (see Scott 2001a), where seniors help other seniors, could be extended to include e-finance.

This leads to a discussion of the roles governments can play in this process. For instance, governments could modify various Acts so that organisations can work together to provide consistent interfaces/solutions, so that confusions and the requirements on learnability, memory and cognitive load are reduced.
**Tiers of government**

Services and websites need to start focusing on customer group needs, rather than delivery according to departmental boundaries. Best practice is perhaps illustrated in the UK where its Audit Office has a mandate to focus on client groups, not the individual department. Australia needs a national strategy that similarly examines the role government can play across departmental boundaries for "joined up" service delivery to older people. We need to create a connected community, which the current top-down decision making between government tiers does not facilitate. A holistic, macro level approach requires the ability to cross departmental boundaries at federal, state and local government levels. Without this there is a risk that only individual accessibility guidelines, for people with certain disabilities, will be considered by disparate departments, and wheels go on being reinvented.

The conflicting agendas, delineation of boundaries and the brochure rather than user-friendly nature of government websites is illustrated by Singh (2002) in attempts to locate appropriate residential care for an 81 year old woman, and by a University of Technology Sydney audit (Dearne, 2002) of NSW government websites.

**Conclusion**

The 'e' in e-commerce is for electronic, not for exclusion. HREOC President Alice Tay points out that “human rights issues arise when people are excluded from services, information or opportunities because of avoidable barriers to access, rather than simply choosing not to participate” (Tay, 2001).

A holistic, macro level approach to the needs and values of older people requires the ability to cross government and departmental boundaries. What is also needed is commitment by the financial sector and equipment suppliers to make sure that the new e-banking standards are adopted and that there are transparent processes for monitoring progress, remedying problems and dealing with complaints. Laudable as the NAB project is to introduce voice-activated ATMs, this only addresses the needs of a few. Holistic, macro level social responsibility needs to consider the perceived needs of the ageing, as expressed in the values discussion above. This will pay digital dividends not only for the ageing in the community now, but also for you the reader, who like all of us increases in age with the passing of each day.

**References**


Australian Bureau of Statistics (2001a) Population by Age and Sex, Australian States and Territories, Cat No 3201.0. Canberra, December 2001


Australian Bureau of Statistics (1999) Special Article - Older Australians [article reproduced from Year Book Australia, 1999, ABS Catalogue No. 1301.0, online at www.abs.gov.au


Doing Ethics: a universal technique in an accessibility context

Christopher R. Simpson¹, Liddy Nevile², Oliver K. Burmeister³

¹Adjunct Teaching Fellow, School of Information Technology, Swinburne University of Technology, Australia, E-mail: csimpson@swin.edu.au;

²E-mail: Liddy.Nevile@motile.net;

³Swinburne Computer-Human Interaction Laboratory, School of Information Technology, Swinburne University of Technology, Australia, E-mail: oburmeister@it.swin.edu.au;

Abstract
Thinking ethically is difficult without a background in moral philosophy. Asking people to embrace ethics without offering practical explanation of the efficacy of so doing, is a thankless task. A technique that people can follow easily, that helps them value ethical behaviour is needed. Illustrations of such a procedure show how professional scenarios are used in the domain of web accessibility. Scenario design and extensions to the technique are considered.

Keywords: Ethics; Accessibility; Case-studies; Dilemma resolution, IT.

Introduction

Whether a student, a retiree or in professional practice, today one confronts many situations where it would be helpful to have a particular way of sifting through issues to determine appropriate courses of action.

Gordon Preece (2002) writing on a recent topical issue put it this way: '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.'

This paper gives the background that gave rise to this technique, the process itself, and then makes use of exemplary scenarios to illustrate how the procedure can be useful to practitioners. One scenario illustrates the approach, while a second illustrates the value in designing appropriate scenarios. The paper ends with suggestions of how the technique, first used in a student context, can be extended to suit professionals from different disciplines as multi-disciplinary teams engage in activities such as building websites.
Background

At Swinburne University of Technology, 'Professional Issues in Information Technology' (PIIT) is taught to all final year IT students. It can be taken by students from other faculties as an elective, although students without industrial experience are strongly discouraged from taking the subject. Over the past 12 years, as the subject has evolved, the focus has been to explore real cases that will confront young (and not so young) professionals in the workplace. This is achieved by having about half the lectures led by industry speakers, as well as through tutorial work, debate and discussion that explore cases collected over the years, and draw heavily on the Industry Based Learning (IBL) experiences of the students.

Students have often expressed difficulty in thinking through ethical situations. PIIT is usually the only subject requiring this in their computing courses. Despite their lack of familiarity with this type of work, 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.

To overcome students' initial difficulties, a simple approach to scenario analysis has been developed. Formative feedback during the semester from tutors has often involved answering student queries in terms of this process, getting them to think through pertinent issues. Similarly, summative assessment has shown that critical thinking and meaningful consideration of multiple alternate solutions to derive a best fit, most frequently occur when this approach is adopted by students.

Although the technique was developed for student use, it is not limited to this context. In the view of the authors, it is widely applicable. To illustrate this point, the scenarios below offer a professional Internet developer's viewpoint, with the technique applied as though carried out by professional peers.

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. The following questions, in this order, have been found to work best (through trial and error over many semesters).

- 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?

Benefits

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 IT
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, at least for PIIT students. 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 appropriate within (or at least independent of) personal belief systems.

**Limitations**

The best results obtained in the PIIT classes have been when the technique has been used in tutorial groups, rather than have students submit individual reflections on particular cases. Individual reflection yields significant results and students have voiced their delight at being able to work through difficult situations using this technique, but even so, further insights and better solutions are derived when it is used in a group situation. Solving scenarios collaboratively also adds credibility to the process, in that much of the professional development takes place in multidisciplinary teams. And that creates new a problem – which ethical standard should one adopt? In multidisciplinary teams, professionals often belong to different professional societies, each with similar, but not identical, codes of ethics. In a student context this leads to interesting discussions, in a professional setting it may lead to conflicting standards that are difficult to resolve.

Another limitation is objectivity. One advantage of thinking through cases, such as those below, before being confronted with real situations, is that it becomes easier to be objective. When confronted with an ethical dilemma in real life, subjectivity can prevent one from being able to make the most appropriate judgments. This is where reference to one's peers, co-workers or members of one's professional society can be helpful. Such people can use this technique to work objectively through the issues and advise the person in the situation of the most appropriate course of action.

**Illustrating use of the technique**

Educational suppliers, world-wide, are depending upon their belief in the commodification and commercialisation of education to offset the increasing cost of education. Typically, they look for or develop learning object repositories and skeletal structures or ‘skins’ within which to serve up compilations of bite-sized pieces, custom-built for individual needs. This form of education could benefit those with disabilities at least as much, if not more, than others. Such disabilities can take the
form of physical or mental human disabilities, or resource or location based incapacities. This is the context of the first case.

**Case 1: Universal access**

*Government funding has been given to a university consortium establishing a repository of resources for school teachers. They have engaged you to develop a search facility for teachers who will use it to discover small chunks of useful material, located anywhere. The chunks will be strung together to make customised lessons for students who cannot attend school, for one reason or another, or whose teachers do not include specialists in subjects the students want to study. The client group knows that it is more 'attractive' to their funding agency if there is a lot of multimedia product in the selection. You know that it is hard to produce accessible multimedia and there is hardly any 'out there'. You are asked to advise your client about accessibility.*

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

- I report to the university consortium.
- I am to develop a repository search facility for school teachers to extract useful teaching materials to develop suitable lessons.
- Target students are supervised by non-specialists (possibly remotely, at home, or in care).
- The government funding agency likes multimedia
- Accessible multimedia content is scarce and 'hard' to develop.
- The consortium requires ‘accessibility’ advice.

**Q2 What are the issues?**

- What are the contractual details/arrangements?
- Accessible multimedia may be costly to develop. There appears to be a funding bias towards multimedia content. How much multimedia is envisaged? Would a simple multimedia put funding at risk? Advice to the consortium might be rejected (along with this job) by recommending a simple, 'non-glossy' approach.
- What are the exact requirements for the multimedia? What standards are to be applied? What is the budget for it and how much of that is for the extra accessibility work?
- Sophisticated multimedia is unlikely to be easily accessed/afforded by all supervisors or students due to special needs and telecommunications inequities.
- What range of resources do supervisors/teachers and students have ready access to?
• What range of disabilities do the target students suffer, if any? How will these be identified and accounted for?
• What level of training and support is envisaged for teachers, non-specialist supervisors and students?
• It is not clear if 'normal' school teachers are to benefit from this system.

Q3 Who is affected?

Adversely…
• My team, if our carefully considered recommendations are 'too pedestrian' and so rejected.
• Students with disabilities, if systems are badly designed or too costly.
• All students, if the system is too cumbersome (costly, slow or otherwise hard to use).
• All students, if the resulting lessons are inadequate, trivialised or unsupported.
• Teachers (particularly non-specialists), without sufficient opportunities (time, funds, help or equipment) to learn about and receive prompt, ongoing support with the system.
• All those unjustly excluded from the system, through negligence or economics or whatever.
• The consortium (and every party concerned), if the system fails, for any reason.

Positively…
• Everyone (including the community), if the job is done with transparency and integrity.

Q4 hence, What are the ethical issues and implications?

• Commitment, integrity and mutual trust between all stakeholders.
• Clarification of project intentions and removal of political bias by the funding agency and consortium, and transparency in discussions regarding advice supplied to them.
• Realistic definition of project scope, based upon: professional design, ethical prioritising of need, provision of sufficient ongoing support.
• Discovery of the real needs of targeted teachers and students.
• Strenuous avoidance raising false expectations.
• Maintenance of sufficient quality of teaching material.
• Particular attention to support of non-specialist teachers.
• Particular attention to support of students with disabilities.
• Particular attention to matching technical sophistication with affordability and accessibility.

…Without attention to the above points, the project cannot proceed successfully, many people and reputations will be hurt, and precious funds will be wasted.
Q5 What can be done about it? - What options are there?

- Advise the client that you need to know more but suspect that this contract will need to specify high standards of accessibility 'in case' there are students or teachers with disabilities as it is almost impossible to make inaccessible content accessible retrospectively.
- Advise them to:
  - Undertake extensive feasibility studies and exhaustive prioritisation before development.
  - Identify the primary beneficiaries of the system.
  - Build in mutual safeguards to help alleviate unforeseen problems.
  - Ensure the ongoing viability of the resulting resource by having sufficient support services.
  - Avoid over-sophisticated technology unless it is clearly affordable by targeted users and disadvantages nobody.

Q6 Which option is best? – and Why?

- In this case, there are still too many unknowns for a decision to be made so the best advice will have to be about what needs to be discovered and how, so that such a decision can be based on informed criteria.

Scenario design

Case studies have frequently been employed to illustrate ethical principles and particularly conflicts and prioritisations amongst those principles. For instance, Anderson et al. (1993) employ scenarios to explore the application of a new code of ethics in different professional settings. Clement (1993), in writing up experiences in a Computer-Supported Cooperative Work workshop, found that discussing scenarios was a productive means to exploring privacy issues. Similarly, Burmeister (2000) used case studies to illustrate the application of the Australian Computer Society (ACS) Code of Ethics to professional practice.

Why design and explore scenarios? Why not just wait until one is confronted with an ethical dilemma in the workplace and then apply the above technique? There are several reasons. In general terms there is the advantage of using scenarios to explore situations ahead of time, while one can engage objectively in the discussion, without a subjective involvement in a particular situation. More specifically, in the accessibility context, scenarios help to identify one's knowledge. Considering accessibility, there are many factors that should be taken into account, as is seen in the discussion above regarding Case 1 and in the discussion about possible extensions to the technique of ethical analysis that follows. Similarly, in other contexts, scenarios can be employed to explore one's knowledge of a particular domain. By asking people what they would do in a particular situation, one can readily identify the limits of that person's knowledge.
For the purposes of ethical scenario analysis, scenarios should be neither self-evident nor simple. Instead, there should be ambiguities that require moral reflection, leading not always to a 'right' solution, but rather towards a solution that is satisfactory. As stated in the limitations above, further reflection by others should yield alternate and perhaps even better solutions than those suggested by the original participants in the discussion. Similarly for Case 1 above, this process gives rise to possible solutions, it does not necessarily lead to the best or even to a good solution. But it does guide people to consider broad, complex issues in a systematic fashion. It is a useful instrument or framework for ethical decision-making.

Another use of scenarios can be to raise awareness of issues. For instance, with little re-working, the two cases in this paper could be phrased so accessibility issues are inconspicuous. Then, in an audience of web designers, the discussion can be used to raise awareness of accessibility considerations, through simple 'what if' additions … What if a user was visually impaired? What if a deaf person tried to access the video clip?

Case 2: Conflict of interest

Australian government sites were mandated to conform to at least single 'A' level of the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) standards, by the end of 2001, seen as best practice in Australia (Sampson-Wild and Burmeister, 2001). Yet the recent call for tenders to audit compliance of government sites, which closed 20th June this year (Innes, 2002), is likely to find very few government sites complying with these standards. The following case assumes your organisation was the successful tenderer …

Your client is a local government agency. You have been asked to develop an accessibility assurance strategy as part of a preliminary contract. You are keen to pick up the contract to build whatever you convince the government to do about accessibility testing, so you are wondering what to recommend. You realise that the agency wants to be told that its materials are accessible, rather than the converse, so you are wondering how high to set the bar for accessibility. You know there are automatic checks available for all the 508 requirements. You could not afford to offer to do all the manual checks required by the WCAG and anyway, suspect the agency's materials would not look good if tested by WCAG.

Like the earlier case, this one has multiple facets with no easy resolution. Recent scandals in the US have involved large accounting firm practices where auditors also have consulting roles, creating a conflict of interest that has caused various now well-publicised problems. Such conflicts are not peculiar to accounting, as is seen in this case.

As mentioned above, one use of scenario design is to explore the domain knowledge of participants. Both cases above involve the government. This was a deliberate, because it raises questions about the applicability of legislation concerning accessibility. Also, in the 2nd case, are legal implications which can either be teased out by a facilitator or left to arise naturally in discussion by participants querying
'WCAG' or '508'. Thus, there is the possibility to discuss the boundaries between legal and ethical considerations. More is made of this point below.

**Extending the technique: from student to practitioner**

The technique began in a student context, but to be more suitable for professionals, it should be extended. IT work today brings together people from different disciplines. This is especially common in complex systems design, typical when building websites. The multi-disciplinary requirements of professionals might better be met with some additional modifications. The *extensions* begin to apply at question 3…

**Q3 Who is affected?**

There are some situations in which, in addition to asking 'who' is affected, it may also be appropriate to ask how the 'environment' is affected. Further, this need not be limited to the 'environment' outdoors, but could also refer to workplace culture, the connectedness of a community, or other situational circumstances.

As stated above, it is significant the government is mentioned as the use of government funding or publication by the government may change the potential liability of the developers and publishers.

Another environmental consideration in Case 1 involves small rural schools that cannot afford specialist teachers, given their small class sizes. In that case, other kinds of accessibility considerations come to the fore, especially in terms of telecommunications access. Low bandwidth might have implications in Case 1 on the type of multimedia design. For instance, high-quality images, ideal for high-speed transmission, might not be appropriate. If a rural student is also disabled, then that further complicates the issues. One frequently employed multimedia technique involves the use of 'chat' environments, yet rural students with disabilities would possibly be totally excluded from participation in such class activities.

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

This question could be extended to include the following three sub-questions:

- What would be 'the right thing' to do?
- Who/what suffers if you do not do the right thing?
- What additional costs will be incurred if you do the right thing?

Doing 'the right thing' is a principle that is often cited in the US and is akin to 'setting a good example', or observing 'best practice'. 'The right thing' is not always the most economical, the fastest or the easiest thing to do, but it is valued for its ethical advantage. Given the wide acceptance of the right thing in some circumstances, it has also come to mean 'that which will have the most beneficial long-term as opposed to immediate effects'.
Q6 Which option is best? – and Why?

This question could be extended to include the following sub-question:

- Who gains if you do the right thing?

Political advantage comes in many forms. It does not always coincide with economic or social advantage. Understanding the potential for bias among the stakeholders can help evaluate potential decisions.

- And Why?

This inevitably casts one's view into the future, where the consequences of our decision will be thrust upon our successors and children, and their environment. Will our decision be seen as wise and far-sighted?

Multidisciplinary extensions

The following two additional questions are inappropriate in the student context, because rarely do IT students have sufficient experience during or prior to their courses to deal adequately with these issues. Typically, the ACS's Code of Ethics requires professionals to consider the legal ramifications of their work on their employer, their clients and the eventual users of the products. But when ACS-accredited professionals work with professionals from other disciplines, they often find that ethical codes of behaviour differ in trivial, or significant, ways and have to make decisions about which 'ethics' to follow. In other contexts, there may be practical considerations to deal with.

The technique could be further extended to include:

- What does the law say?
- What chance is there it will be enforced?

Particularly in web site development, where cross-border business is concerned, legal compliance becomes a complex issue. The cases above show that compliance in one jurisdiction does not imply one's product complies in another. For instance, there are subtle differences between complying in Australia with the accessibility requirements for Australian government sites, and compliance requirements for the same sites, in the US. In Case 2, mention of particular standards (WCAG and 508) are introduced to lead participants to focus on relevant legislation.

Conclusions

Though this technique evolved out of the need to help students think through ethical dilemmas in a systematic way, it is not limited to a student context. The process will work just as well in peer evaluative situations. For instance, one of the limitations referred to above is that when confronted with an ethical dilemma in the workplace, it is difficult to remain objective in one’s analysis. In such a situation, this technique
will help a knowledgeable peer/co-worker to work objectively through the issues to develop appropriate advice on how best to proceed. Similarly, members of the ACS are encouraged, when confronted with ethical dilemma, to seek help from the society and/or from the Australian Institute of Computer Ethics (AiCE). People who are asked for advice need a way of sifting through the pertinent issues to devise an appropriate response. The ACS Code of Ethics goes part of the way to do this. Yet it really only sets the standard, as it does not provide a way of arriving at the best (or at least a satisfactory) solution. What has been proposed in this paper is a recipe for formulating such a solution.

Further work is needed to validate the technique. At this time, there is only anecdotal evidence from tutors involved in formative and summative assessment of student work, and from students themselves. There is also anecdotal work that supports the value of such scenarios when trying to alert practitioners to the problems of accessibility, and when working towards recommendations for action in response to those who request help from AiCE members. Formal data needs to be gathered as to the efficacy of this technique for isolated practitioners, as well as to enhance it, if possible.

References


Killer Robots

Robert Sparrow,
Centre for Applied Philosophy and Public Ethics,
Department of Philosophy, The Old Quad,
University of Melbourne, Victoria 3010. Australia.
Email: rsparrow@unimelb.edu.au

Abstract
The United States Army’s Future Combat Systems Project, which aims to manufacture a “robot army” to be ready for deployment by 2012, is only the latest and most dramatic example of the military interest in the use of artificially intelligent systems in modern warfare. A number of “autonomous weapon systems” (AWS) are already in use in armed forces around the world, including robot surveillance drones, robots for urban reconnaissance, cruise missiles, torpedoes and submersibles, and more are in production or on the drawing board. The military remains one of the largest sources of funding for research into robotics and artificial intelligence technology. As these technologies improve it seems inevitable that they will be used more and more in warfare.

This paper considers the ethics of the decision to send artificially intelligent robots into war, by asking who we should hold responsible when an autonomous weapon system is involved in an atrocity of the sort that would normally be described as a war crime. A number of possible loci of responsibility for robot war crimes are canvassed; the persons who designed or programmed the system, the commanding officer who ordered its use, the machine itself. In fact none of these are ultimately satisfactory.

The designer or programmer of a robot involved in a war crime could only be held responsible if the actions of the robot reflected negligence on their part. But this need not be the case. Any device capable of learning from its environment or experience may act in ways that its designers cannot predict. The most natural place to locate the responsibility is with the commanding officer who ordered the use of the weapon. However this move too sits uneasily with the claims made about the “autonomy” of such systems. The more these machines are held to be autonomous then the less it seems that any human being can be held responsible for their actions.

This leaves the machine itself. But it is exceedingly difficult to imagine holding a machine responsible for a war crime. I explore why this is the case by drawing our attention to the link between moral responsibility and the possibility and appropriateness of punishment. We cannot hold that a machine was morally responsible unless we could punish it if we found it guilty of a crime. The possibility of punishing a machine in turn requires that machines can properly said to suffer. I argue that it will not be possible to hold that machines can suffer until they develop expressive capacities akin to those of living creatures, and offer some considerations which suggest that this is a much more demanding requirement than is generally
realised. For the foreseeable future it will not be possible to punish machines or, therefore, to hold that they are morally responsible for their actions. It is a necessary condition for fighting a just war, under the principle of *jus in bello*, that someone can be justly held responsible for deaths that occur in the course of the war. It will therefore be unethical to deploy autonomous systems in warfare unless someone can be held responsible for the decisions they make where these might threaten human life. The more autonomous these systems become, the less it will be possible to properly hold those who designed them or ordered their use responsible for their actions. Yet the impossibility of punishing the machine means that we cannot hold the machine responsible. We can insist that the officer who orders their use be held responsible for their actions, but only at the cost of allowing that they should sometimes be held responsible for actions which they could not reasonably have been expected to foresee and over which they had no control. The deployment of autonomous weapons systems in warfare is therefore unfair either to potential casualties in the theatre of war, or to the officer who will be held responsible for their use.
An Examination Of Non-Business Usage of the World Wide Web in Two Western Australian Organisations

Craig Valli

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
Email: c.valli@ecu.edu.au

Abstract

This is an examination of 2 cases in an ongoing research project into the misuse of the World Wide Web in the workplace. OrganisationA is a large University department and Organisation B is a large state government organisation. The paper examines the generic results and gives interesting case behaviours of users within each organisation. A range of behaviours identified by the research is problematic for both organisations. Both of these cases however see pornography as less of an issue than existing literature would lead us to believe. MP3 and streaming video however are the new emergent threat in both organisations.

Keywords - Internet, WWW, abuse, pornography, MP3, misuse, proxy, video

Introduction

Most of the existing literature relating to the level of Internet misuse and abuse is based on limited survey and often blatantly commercial bias (Holtz, 2001). There is often no real attempt to measure or rate the level of misuse or non-business use that does occur within an organisation. These 2 cases are part of on-going research that is attempting to measure the non-business use or misuse of the World Wide Web (WWW) in selected organisations. Non-business use for the data examined in this study will mean any activity on the World Wide Web that is not directly related to fulfilment of a persons job description or is not done in the course of processing a workflow related to their job.

The cases are from 2 large Western Australian organisations. Organisation A is a large University department with 846 unique users and Organisation B is a large state government department with 1946 unique users. Both organisations have large broadband connections to the Internet and supporting infrastructure.

This paper will describe how the analysis was performed, the overall generic results from both cases and then an examination of interesting patterns and behaviours of abusive users.
Method Of Analysis

The log files were analysed by 4 different log file analysis tools these were Cyfin (Wavecrest, 2002), Squid Analysis Report Generator (SARG) (Orso, 2001), Webalizer (Barrett, 2002) and pwebstats (Gleeson, 2002). Cyfin (Wavecrest, 2002) is a commercially available tool that allows for extensive analysis of a wide range of proxy server log files and subsequent adaptation of reports and outputs for analysis. Cyfin allows for a high level graphical reporting of the traffic usage patterns and is used as a tool to look at macro usage patterns. It also categorises traffic into 55 preset categories and 10 customisable categories of URL’s. The preset categories are a set of preselected sites that match certain criteria to be placed into these categories. The log files are then processed and the sites contained in the log files are then categorised. The author used all of the preset categories and created custom categories as necessary for both organisations.

SARG (freeware) and pwebstats (freeware for educational institutions) both have the ability to process log files natively. They both produce general statistics with a high level of granularity making it possible to determine down to the user and file level any activity that is generated. SARG in particular gives a detailed 24-hour histogram of each users traffic usage, which allowed the author to readily analyse hours of web usage by users.

Webalizer does not handle certain log files natively and the log files had to be converted into Common Log file Format (Consortium, 1995) using a perl based script. Webalizer allowed for a reasonable degree of granularity but it was not as comprehensive as the SARG outputs. It did however confirm general statistics generated by the other log file processors on a user and overall basis. All log files were run initially through Cyfin to attempt to find any macro patterns of behaviour. Then using the Cyfin data as a guide the other tools were used to examine the log file data in greater depth. For confirmation of generic statistics the log the SARG, Webalizer and pwebstats applications processed files in full.

Generic Statistics

Organisation A

All of the analysers produced the same generic statistics with a transmitted traffic volume of 121GB and total log file line entries of 11 million. They all identified the same top users for the web traffic.

Initial analysis was done with Cyfin as the author was looking for trends and potential macro problems that were occurring with usage. By strictly applying the guidelines for the University 74.6% (90.4 Gigabytes) was unacceptable and 25.4% (30.8 Gigabytes) would be acceptable. The top 15 categories of usage are displayed below

<table>
<thead>
<tr>
<th>Categories</th>
<th>Kbytes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downloads</td>
<td>29,783,299</td>
<td>24.6%</td>
</tr>
<tr>
<td>Multimedia</td>
<td>23,761,296</td>
<td>19.6%</td>
</tr>
<tr>
<td>Hardware and Software</td>
<td>14,015,702</td>
<td>11.6%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>6,205,800</td>
<td>5.1%</td>
</tr>
<tr>
<td>Categories</td>
<td>Kbytes</td>
<td>%</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>Multimedia</td>
<td>61,118,745</td>
<td>42.8%</td>
</tr>
<tr>
<td>Banners/Ads</td>
<td>11,905,985</td>
<td>8.3%</td>
</tr>
<tr>
<td>Downloads</td>
<td>9,460,292</td>
<td>6.6%</td>
</tr>
<tr>
<td>News and Media</td>
<td>8,336,045</td>
<td>5.8%</td>
</tr>
<tr>
<td>Hardware and Software</td>
<td>8,174,237</td>
<td>5.7%</td>
</tr>
<tr>
<td>Sports</td>
<td>7,941,328</td>
<td>5.6%</td>
</tr>
<tr>
<td>Government</td>
<td>6,672,905</td>
<td>4.7%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>6,414,616</td>
<td>4.5%</td>
</tr>
<tr>
<td>Internet Services</td>
<td>6,066,964</td>
<td>4.2%</td>
</tr>
<tr>
<td>Email</td>
<td>5,806,737</td>
<td>4.1%</td>
</tr>
<tr>
<td>Reference</td>
<td>5,010,673</td>
<td>3.5%</td>
</tr>
<tr>
<td>Financial</td>
<td>4,822,891</td>
<td>3.4%</td>
</tr>
<tr>
<td>Search Engines</td>
<td>3,115,315</td>
<td>2.2%</td>
</tr>
</tbody>
</table>

**Table 1 – Usage by Categories Organisation A**

For the log files examined only 13 users out a total of 846 (1.6% of users) were responsible for consuming over 50% of this bandwidth, 56 users (6.6% of users) used 75% and the remaining 750 users used the remaining 25% of the volume for the period examined.

**Organisation B**

All of the analysers produced the same generic statistics with a transmitted traffic volume of 142.8GB and total log file line entries of 27 million for the period 1st January 2002 until 16th June 2002. Initial analysis was again done with Cyfin as the author was looking for trends and potential macro problems that were occurring with usage. If the policy organisational was applied 56% (80.1 Gigabytes) was Unacceptable and 43% (62.7 Gigabytes) was Acceptable traffic.

The usage per user was more heterogenous in this organisation with the top 50 users consuming only 41.2%(58.3 Gigabytes) of traffic. If the 2 heaviest users who were the IT staff downloading legitimate service packs and updates this drops to 35.7% (51.1 Gigabytes) of traffic is used by the top 50 users. The top 15 users in this organisation except the IT staff consumed 18.8%(26.9 Gigabytes) of traffic which again could be indicative of abnormal or abusive use of the WWW.
<table>
<thead>
<tr>
<th>Society and Culture</th>
<th>2,754,390</th>
<th>1.9%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Estate</td>
<td>2,736,462</td>
<td>1.9%</td>
</tr>
</tbody>
</table>

Table 2 – Usage by Categories Organisation B

This organisation has an extremely high usage of multimedia that accounted for over 42% of all the bandwidth consumed by the organisation. The next highest category by usage was Advertisements and Banners at 8.3% of bandwidth.

Selected Examples Of Misuse

OrganisationA – The Unwitting Abusers
Both users displayed behaviours that can only be considered as abusive and inappropriate usage of the resources. Combined they used 20 Gigabytes of traffic volume throughput for the cache although they did not directly download a large percentage of the traffic from the Internet.

The users who generated this traffic could be described as a non-malicious user or a user highly ignorant of bandwidth issues. Of the some 11263Mbytes User1 put through the proxy server, 10151Mb of this traffic was video based traffic. User2 produced 8502Mbytes of traffic of which 8002Mbytes was video based traffic. The fact that this traffic was on the internal LAN running across a 1GBit backbone to 100Mbit at the desktop should have not presented an issue if it was normal network traffic. However, the fact the camera would have effectively bombarded the cache memory on the Squid proxy caching server has some severe implications for cache serving ability. To further compound the problem the content being sent on web camera occurred within 31 hours over 5 days typically in peak usage times for other legitimate users.

One of the main problems is the volume of traffic that this activity would have generated. In the top 8 hours the usage, was around 10Gbits of network throughput per hour. This extra traffic would have meant that the cache would have been severely hampered in its ability to service legitimate traffic due to this additional loading. The traffic was streaming video and the number of cacheable objects that this generated was also extremely high.

The effect on the cache would have been that it would have flushed legitimate objects off the cache on the disk and also out of the cache memory of the caching server. By doing this any benefit gained by using a cache would have been lost. It would have also meant that several gigabytes of already cached relevant and reusable objects would have been flushed out of cache.

OrganisationB – Mandrake but No magician
The highest user of the bandwidth excluding the 2 identified IT staff was a user who consumed 2.64 Gigabytes of volume. Of which 1.8Gigabytes was consumed in March 2002 with 1.5Gigabytes of this being the Mandrake Linux ISO images for installation. The remaining bandwidth was primarily consumed via the download of MP3 and MOV files for either viewing or listening to. Over 90% of the activity of this user was against established policy.
OrganisationA - The Nightstalkers
There was 15888Mbytes of data that was accessed by these users through the proxy server. It was found that 90% of this traffic was unacceptable and not adhering to the acceptable usage policy of the OrganisationA. A high proportion of that 90% was downloading and viewing streaming media whether they were pirated versions of new release movies, pornographic movies or song files.

Users accessing this material were doing so during hours where the only potential for detection is essentially in an audit of the log files. This behaviour would indicate that the users are aware that their behaviour is potentially abusive even though they maybe unaware of the organisational acceptable usage policy. Furthermore the fact that they are potentially breaking several criminal codes by commissioning of these activities would further add levity to this argument.

User3 downloaded 7242 Mbytes of traffic of which, 5357 Mbytes or 74% of bandwidth consumed was streaming movie files in particular the .ASF format. Of the remaining bandwidth 1652 Mbytes were MP3 song files of MPEG and AVI based pornographic movies less than 300Mbytes could be classified as legitimate traffic in this case.

The user perpetrated most of these accesses between the hours of 11pm and 6am. This usage on the 2 worst days was 2762 Mbytes on a Wednesday and Thursday in December that is well out of standard working times. There were only 19 hours idle out of the 48-hour period of accesses. The accesses during this period were a smorgasbord of sex, sound and cinema.

User4 downloaded 4020 Megabytes of data from the proxy of which 89% or 3522 Mbytes was unacceptable traffic. This user was more dedicated to the download of streaming media be they movie files, pornography or MP3 song files.

Of the remaining 498 Mbytes, there was 170Mbytes of email traffic, which is large when these users are provided with conventional POP3 accounts for email. What is of even further interest is almost 45MB of chat traffic, of which approximately 1800 visits were to chat sites. What makes this figure large is that the user was only generated this traffic in 295 hours, which equates to 6 visits per hour to a chat site. The inappropriate accesses by this user were once again perpetrated mainly during the hours of 11pm and 6am. The accesses by this user though were more evenly spread and showed a consistent rather than erratic pattern of misuse.

The analysis for this User4 followed similar patterns with almost 3200 Mbytes of traffic dedicated to the download of movies and MP3 files. The behaviour patterns of waiting until the small hours of the morning to perpetrate much of this abuse were also demonstrated in the log file analysis reports.

OrganisationB – The Need for Speed
This user was primarily accessing motor racing sites and some Sony Playstation related games sites and had a volume usage of 2.01 Gigabytes for the period examined. This involved the regular viewing of the sites amounting to visits 10 - 20 times a day. In this users standard behaviour pattern was the downloading of various trailers and video clips from these sites either demonstrating the latest games available
or live footage of car racing related activities. The non-business usage in this case exceeded 95% of the volume downloaded by this user.

*Organisation A - User 6 – Risk Taker*
User 6 had what appears to be a modest 1623Mbytes of bandwidth of which 1200MB was downloading of patches for their systems all legitimate traffic however this is where it ends. The remaining bandwidth while only 423MB is very problematic. MP3 and movie traffic accounted for 190Mbytes of this 423MB, which is against policy, and some of the traffic was in direct breach of copyright. Of the remaining non-legitimate traffic analysed pornographic traffic accounted for 45MB of this activity. What made this case even more problematic was that User 6 had paid memberships to several hardcore pornographic sites that they were accessing from the organisations connection providing a further audit trail for this activity.

A potential productivity issue was that User 6 had a high number of requests to a stock market quote engine on the web that accounted for 7.45% of their time. The rest of their surfing pattern accessed a wide category of sites representing 26 different categories from a selection of 55 in the Cyfin (Wavecrest, 2002) analysis tools set of base categories and presented no real problem.

*Organisation B – The User has left the Building*
The eighth highest user of bandwidth in Organisation B did so in the first 2 months of the year. The staff member left the employ of Organisation B as the bandwidth consumed stopped on Friday 22nd February and was later confirmed with the organisation. The total downloaded was 1.50 Gigabytes the traffic usage accelerated in the last few weeks and over 90% of the traffic was downloads either full programs or updates to various shareware or freeware offerings.

**Discussion Of Analysis Of Log files**
The analysis of the results in both organisations highlighted the ubiquity of MP3 and video based traffic. This traffic apart from the fact that it is against established policy for users to be generating this sort of traffic is a major risk in terms of copyright violation. Many of the MP3 and video files downloaded were pirate copies of original works. In addition to the downloading of these files it appears that some of the users were arming themselves with a variety of utilities to be used to record the downloaded files to CD-ROM for possible later use/or distribution. Organisation B in particular has a large problem with over 50% of downloaded volume constituting MP3, MOV or video based streaming traffic.

Both organisations have provided users with static email accounts that they are expected to use for their e-mail traffic. Yet both organisations have considerable bandwidth being used to access and transmit email via web based e-mail systems. Organisation B has users consuming over 7 Gigabytes of volume through these activities, Organisation A over 6 Gigabytes which is approximately 5% for both Organisations. If both organisations are providing standard email services and clients to users this raises several points. What is the motivation behind using these systems is it convenience or the fact they do not wish to send the types of emails they are sending via the WWW across standard systems for issues of privacy or avoidance.
The behaviour of the departing staff member in OrganisationB also raises issues for serious consideration for new procedures for access to IT resources for staff that have given notice. The user in this case accelerated their use of the WWW in the period post notice and prior to them leaving. This could indicate that the major behavioural modifier for the organisation policy i.e. the threat of retrenchment for inappropriate use of the WWW is perceived to be null as they the user are leaving the organisation.

Not all of the traffic analysed had malicious or abusive implications in both organisations. In fact the largest detected misuse of the proxy was that of the 2 users who unwittingly placing a video camera on the network in OrganisationA. This generated sufficient traffic over five days during peak usage periods to overload the proxy server to such a point it would have hampered legitimate use of the Internet connection for other users.

The downloading of pornographic material, although not large in volume when compared to other traffic, does however represent a potential problem for OrganisationA. The users who were accessing this sort of material were doing so at times where detection of this activity would be highly unlikely except in case of an audit of log files. The volume of material that the users downloaded, coupled with the fact that they requested some of these files more than once from the system, would indicate possible problem behaviours on their part. OrganisationB’s detected pornographic traffic was less than 300MB or 0.2% of all traffic by volume and less than 0.001% by request and as such does not represent a problem. Further compounding problems for OrganisationA was User6 who is a paid member to several hardcore pornographic sites who is deliberately accessing these sites during their working day in breach of existing policy and potentially jeopardising their employment. The actions of the User6 are further brought into question when 7.5% of their surfing time is spent requesting quotations from an on-line stock quoting facility. Which means that at least 7.5% of the time during the normal working day they are doing something other than they should be.

Some of the commercially available abuse detection tools failed to effectively detect abuses by the users from a different linguistic and cultural background. The software failed to detect and appropriately categorise many Southeast Asian sites and in particular MP3 and pornographic web sites which some of the abusers frequently visited in OrganisationA. This appears mainly due to many of the undetected sites containing native language in their URL’s. Previous study of similar issues by (Hunter, 2000; Nunberg, 2001; Weare & Lin, 2000) have found shortcomings in content filtering technologies reliability at detecting inappropriate content. The problem of non-English websites uncovered in this case would indicate that there are further difficulties with relying solely on a content filtered approach to your web content management. OrganisationB deploys Cyber Patrol a content filtering package, which would seem to have been effective at reducing pornography but that organisation had the highest usage of MP3 and Multimedia related sites, which is just as problematic. Many of the URL’s that escaped detection by Cyber Patrol i.e. they allowed download of material were picked up by Cyfin which categorised material which lends weight to the argument for an eclectic use of tools for the prevention and detection of misuse within an organisation.
Conclusion

The 2 cases have demonstrated that in plain monetary terms for bandwidth provision (based on pricing of $200 per Gigabyte delivered) non-business use is costing Organisation A approximately $54,000 per annum and Organisation B it is cost approximately $32000 per annum alone. These are the apparent costs what of hidden costs of lost wages, wasted resource and lost business opportunity due to poorly performing Internet links.

The 2 cases have produced some implementation issues that need further consideration and examination. Firstly, how effective are current content management systems at detecting inappropriate usage when used in isolation. Do cultural and linguistic factors affect the ability of these content management countermeasures even with the WWW having a heavy English based bias in content?

Have MP3, MOV, AVI and other streaming video and audio technologies possibly overtaken pornography as a risk and liability issue for organisations accessing the Internet? Is most of the significant abusive use of the World Wide Web perpetrated in organisations done so by a small percentage of the user base? What effective policy measures if any can protect against staff that are leaving your organisation abusing their WWW access? Why are staff using web based email services when they are provided with standard mail services in the workplace?

The issues raised are not easily answered and warrant further investigation for us to start to understand how organisations and their respective user bases are using or misusing the WWW.

References


Australian Hackers: an Ethical Perspective

M.J.Warren* and W.Hutchinson†

*School of Information Technology, Deakin University,
Geelong, Victoria, Australia.

†School of Computing & Information Science, Edith Cowan University,
Mount Lawley, Western Australia, Australia.

E-mail Contact: mjwarren@deakin.edu.au

Abstract

The aim of the paper is to look at the way hackers act and ways in which society can protect itself. The paper will show the current views and attitudes of hackers in an Australian context. The paper will also include a case study to show how a hacking incident can develop and how technology can be used to protect against hacking.

Keywords: Computers and Society, Australia, Hacking

Introduction

We have seen a rise in computer misuse at a global level, it is generally thought that ‘Hackers’ are responsible for these attacks. Hackers are perceived as being adolescent males, in dark bedrooms being able to cause massive damage across the world just by the use of their computers. A more romantic perception portrays them as being determined: cyber knights with a code of conduct to live by just like the great Arthurian knights. This paper looks at hackers, their ethical viewpoint and the role and impact of hackers within Australia.

Computer Hacker - The Definition of Hacking

According to Bruce Sterling (1993) in his book titled ‘The Hacker Crackdown’, the term “hacking” is the act of intruding into computer systems by stealth and without permission (Lopez-Fernandez and Warren, 2002). However, this name is used routinely today by almost all enforcement officials with any professional interest in computer fraud and abuse to describe any crime committed with, by, through, or against a computer. Moreover, ‘hacker’ is what computer-intruders choose to call themselves, not as a criminal pejorative, but as a noble title given to those “soaked through with heroic anti-bureaucratic sentiment.” (Sterling, 1993). Hacking then, can describe the determination to make access to computers and information as free as possible. Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and the spirit (Levy, 1984).
State of Australian IT Security and Australian Hackers

A recent AusCERT Survey (Auscert, 2002) has focused upon the state of IT security within Australia, the following is a summary of the main results:

- 67% of all organizations surveyed have been attacked in 2002 - twice the 1999 level and 35 per cent of these organizations experienced six or more incidents;

- 98% of companies had experienced either computer Security incidents / crimes or other forms of computer abuse (such as network scanning, theft of laptops, employee abuse);

- Of Australian organisations who were victims of computer incidents, 65% of these attacks were from internally parties within the organisation and 89% came from external sources;

- 43% of Australian organizations were willing to hire ex-hackers to deal with security issues, three times more than in the US.

The survey showed that IT security and computer misuse are a major problem within Australia. The survey showed that external attacks were the source of the majority of attacks. Perhaps of interest is the willingness of Australian organization to use hackers to improve their security.

Hacker Motivation

A recent hypotheses put forward has been regarding hacking motivation is that they are suffering from Asperger syndrome (Dreyfus, 2002).

Aspies typically have an almost obsessionnal approach to solving problems and are often oblivious to their peers' view that a given problem is ‘unsolvable’. Both are often prerequisites to becoming an elite-end hacker. There does not appear to be any in-depth research linking illegal hacking and Asperger syndrome. However, one of the world's leading Asperger syndrome experts, Australian clinical psychologist Tony Attwood, believes some hackers may share characteristics with "Aspies", as they refer to themselves (Dreyfus, 2002).

"It's the sheer challenge rather than any (criminal intent). It's the pursuit of knowledge and truth - with different priorities and perceptions. They see it as an intellectual challenge and a prize, (and) they look at the success of what they have done rather than the consequences of the lives of people they have affected" (Dreyfus, 2002). Perhaps technology and deception combined into ‘honeypots’ and ‘honeynets’ can offer protection against such individuals.

Honeypots & HoneyNets

A Honeypot is a ‘pretend’ server with the aim of tracking black-hats (an unauthorized person trying to get access to a system) (Spitzner, 2000a) in the act of probing and compromising a system. The aim is to deceive the black-hat into thinking they are
attacking an actual real life server (software examples include systems by Cohen 2000, and Network Associates, 2000). The aim of the honeypot is to monitor the black hats by a number of means (Spitzner, 2000a), they are:

- Tracking the honeypot firewall logs
- Analysis of honeypot system logs to determine what the kernel and user processes are doing.
- Using a *sniffer* on the firewall that ‘sniffs’ any traffic going to or from the honeypot. The advantage of a sniffer is that it picks up all keystrokes and screen captures.
- Using a *tripwire* on the honeypot. A tripwire tells the system administrator what binaries have been altered on a compromised system (such as a new account added to: /etc/passwd, or a trojaned binary).

The aim of the honeypot is to attract the black-hats, monitor them, let them gain root access to the system, and then eventually log them off the system, all without any suspicion being aroused. Once black-hats gain root access, they are monitored for several days in order for the system administrator to learn what they were doing. The biggest problem is how to limit the black-hats offensive actions (Spitzner, 2000b). This is done by using the honeypot firewall, and implementing a rule base schema that allows access from the Internet to a honeypot’s firewall, but limits outbound network traffic. It is important that the black-hat is allowed enough outbound traffic so as not to arouse suspicion.

The results of these honeypot assessments are made public ([http://project.honeynet.org/](http://project.honeynet.org/)) so that network administrators can access the information and ensure that they are protected against common hacker attacks and techniques.

The work by Spitzner developed into expanding the Honeypots into Honeynets. Spitzner (2000c) identified that the honeypots needed to be expanded for the following reasons:

- to be able to determine attacks upon switches, routers and different operating systems of a network
- generate information from several sources (for example, honeypots) in order to provide information in greater detail.
- detect new attack patterns such as vulnerability scanning and how black-hats progress from one system to another.

The result was grouping a number of honeypots together to form a honeynet, so a hacker would feel that they were gaining access to a much large networked system. An ideal solution to stop someone suffering from the Asperger syndrome to cause harm is by the use of honeypots and honeynets.

A major issue is whether the use of honeypots and honeynets are ethically acceptable. Is it ethically acceptable to deceive an attacker who is trying to hack into a computer systems?
Australian Hackers

Research in the early 90’s within Australia showed that computer crime and hacking was a problem. Victoria was the first Australian state to implement state law to outlaw hacking in 1988 and the Commonwealth followed in 1989 (Hughes, 1990). An analysis of computer crime in 1991, showed that within Australia between 1990 and 1991 there had been 497 computer abuse incidents and 31 incidents related to hacking (around 6% of incidents) (Kamay & Adams, 1992). Research at this time also indicated Australian perception towards computer crime was influenced by cultural precedents (Coldwell, 1995). Other studies at this time also looked at the Australian perception of Computer Crime, a study was undertaken looking at teachers’ perception of hacking and found from a sample group that 60.2% thought hacking was unacceptable and 39.8% thought hacking was acceptable (Coldwell, 1994). In 1997 “Underground” was written which described the history of Australian hackers during the early nineties, the development of the ‘Wank virus’ and ‘plans’ to destroy NASA computer systems (Dreyfus, 1997). Since that time, most of the Australian hacking community seem to have disappeared, no well known Australian hacking groups or even Australian hacking conventions are in existence. The only large Australian hacking group is “2600 Australia”, (http://www.2600.org.au/) this group is based upon the famous US hacking group 2600. The philosophy of 2600 Australia is “2600 Australia is a loose-knit group of people interested in computer security, electronic gadgetry, communications and just technology exploration in general” and in terms of their activities can be best described as a computer club. No research has been undertaken to determine the numbers of hackers within Australia. Since the mid nineties there has been no major hacking incidents involving Australia or Australian hacking groups, the Millennium Bug period and Olympic Game passed without any publicized incident.

The most recent famous Australian hacking case was to do with sewage. In October 2001, Vitek Boden was convicted of 30 charges involving computer hacking of the Maroochy Shire Council sewerage system. The attacks, which commenced in late 1999, involved using remote radio transmissions to alter the actions of the sewerage pumping stations and caused hundreds of thousands of litres of raw sewage to be pumped into public waterways (Kingsley, 2002). In the year 2002, does hacking by Australian hackers and hacking groups pose a real problem?

An Example of an Australian Hacking Case

The following is example of a typical Australian hacking case in chronological order. The case study shows how a hacking incident can develop and how the press become focal point (Lopez-Fernandez and Warren, 2002):

Carr defends MP in hacking case (Australian Financial Review 07 Aug 2001)
The NSW Labor MP at the centre of a hacking scandal said yesterday he had once trained as a computer programmer, after initially saying he `'wouldn't know the first thing about hacking into a computer". It also emerged yesterday that the computer of a senior Liberal MP, Mr Peter Debnam, had been unlawfully accessed at Parliament on a public holiday. A computer belonging to the Labor MP, Mr Tony Kelly, was seized by NSW Police yesterday after allegations that confidential files belonging to
the Opposition were found on a computer in the parliamentary office of the State Government's leading Upper House strategist Mr Tony Kelly.

*Office ban on computer MP's son* (Sydney Morning Herald 07 Aug 2001)
The son of the Labor MP at the centre of computer hacking allegations at State Parliament was barred from his father's parliamentary office last month, the Herald has been told. The Upper House MP, Mr Tony Kelly, who admitted training as a computer programmer in the 1970s and 1980s, refused to comment on reports his son had extensive computer skills. It is understood Mr John Kelly has been a regular visitor to his father's office.

*Hacking skills denied* (Illawarra Mercury 07 Aug 2001)
The NSW Labor MP at the centre of a parliamentary computer hacking scandal has revealed he had been a computer teacher at a TAFE college.

*Political espionage* (Sydney Morning Herald 08 Aug 2001)
Sometimes security is only noticed when there is none. The discovery that a State Government MP's office computer may have been used to hack into Opposition computer files has shaken the customary quiet sense of security that pervades parliamentary life.

*MP in hacking affair steps aside* (Sydney Morning Herald 08 Aug 2001)
The controversy surrounding the alleged hacking of an Opposition MP's computer deepened yesterday as the Carr Government politician at the centre of the allegations was forced to stand aside from his parliamentary positions.

*Hacking claims: MP steps aside* (Illawarra Mercury 08 Aug 2001)
The NSW Labor MP at the centre of a parliamentary computer hacking scandal stood aside from his Upper House duties yesterday as the search for the hacker continued.

*NSW Labor MP steps aside during inquiry into hacking* (Australian Financial Review 08 Aug 2001)
The NSW Labor MP Mr Tony Kelly stood aside from parliamentary duties yesterday amid a police investigation into computer hacking at State Parliament.

*Labor MP steps down from duties* (Newcastle Herald 08 Aug 2001)
The NSW Labor MP whose office computer is at the centre of a parliamentary computer hacking scandal stood aside from his Upper House duties yesterday as the police investigation continued.

*Hacking software found in Mp's computer* (Sydney Morning Herald 09 Aug 2001)
A computer in the office of the Labor MLC Mr Tony Kelly was loaded with password ‘sniffing’ software that could have been used to break into the personal files of the Liberal MP Mr Charlie Lynn, a consultant hired to investigate hacking allegations inside the NSW Parliament has found. The Herald has confirmed that the 12-page preliminary report by a Melbourne firm, eSec, commissioned by parliamentary staff and handed to police on Tuesday, recommends a more detailed analysis of the computer files.
Staff kept suspicious software under wraps (Sydney Morning Herald 10 Aug 2001)
The NSW Parliament ‘hackergate’ controversy deepened last night when parliamentary staff revealed they had covered up for nine days the discovery of suspicious software on an MP's computer.

Carr denies Labor not cooperating (Illawarra Mercury 13 Aug 2001)
NSW Premier Bob Carr has denied Labor members were unwilling to cooperate with the police inquiry into State Parliament's computer hacking scandal.

MPs‘ House rules frustrate police hunt for hackers (Sydney Morning Herald 14 Aug 2001)
Police investigations into computer hacking allegations at the NSW Parliament are being frustrated by parliamentary privilege.

Hacker squad get the go-ahead on MPs' files (Sun Herald 19 Aug 2001)
Detectives from the Commercial Crime Agency will return to Parliament House in Macquarie Street tomorrow following a major breakthrough in the computer hacking investigation.

MP clear in hack inquiry (Illawarra Mercury 31 Aug 2001)
NSW Labor MP Tony Kelly was cleared yesterday of any criminal activity by police investigating allegations of computer hacking at State Parliament.

Police clear MP of hacking allegations (Sydney Morning Herald 31 Aug 2001)
The mystery surrounding the NSW Parliament "hackergate" controversy remained yesterday when police cleared the Upper House Labor MP Mr Tony Kelly. They found that there were computer files belonging to Liberal Party MLC Mr Charlie Lynn on a computer from his office.

MP's son admits: 'I loaded software' (Sun Herald 02 Sep 2001)
John Kelly, son of embattled Labor MP Tony Kelly, has told police investigators that he loaded hacker software on to his father's Parliament House computer.

Parliament insecurity (Sydney Morning Herald 03 Sep 2001)
The police inquiry into State Parliament's so-called "hackergate" controversy has done nothing to restore faith in a system that should guarantee MPs unconstrained freedom in representing the public effectively. After a month-long investigation police have confirmed that unauthorised copies of computer files belonging to the Liberal MP, Mr Charlie Lynn, were found on a computer in the parliamentary office of the State Government's leading Upper House strategist Mr Tony Kelly. This is a serious finding…

IT blamed for secret downloads (Sydney Morning Herald 04 Sep 2001)
Questions continue to be raised in the mystery over the NSW Parliament hacker scandal after a report blamed parliamentary IT staff for accidentally loading confidential files belonging to the Opposition MLC, Mr Charlie Lynn, on to the computer of the NSW Labor MP, Mr Tony Kelly.

Kelly no computer hacker (Illawarra Mercury 04 Sep 2001)
NSW Labor MP Tony Kelly has demanded an apology from Opposition leader Kerry Chikarovski after being cleared yesterday of hacking into confidential Liberal Party computer files.

MP's son loaded 'hacking software' (Illawarra Mercury 05 Sep 2001)
The NSW Labor MP embroiled in a computer hacking scandal has confirmed his son was responsible for loading suspect software on his PC.

Revealed: how MP's son used computer in hacking scandal (Sydney Morning Herald 05 Sep 2001)
The son of Mr Tony Kelly, the Labor MP at the centre of hacking allegations, was using a computer in his father's parliamentary office late one Friday night to run software that can scan computer networks for security weaknesses while his father was overseas on parliamentary business.

No evidence of hacking, says clerk of Parliament (Sydney Morning Herald 07 Dec 2001)
The clerk of the NSW Parliament did not contact police after security software was found on an MP's computer because he had no evidence that any offence had been committed, he revealed last night. In a final report on the hacker controversy sparked after suspicious software and files were found on the computer of Legislative Council member Tony Kelly in July the clerk of the NSW Parliament, John Evans, said it would have been inappropriate of him to assume an offence had occurred without independent evidence.

The mini case study shows the main aspects of a hacking crime:

- the actual attack and determination that an attack had taken place;
- the response to the attack by the organisation;
- involvement of legal authorities;
- outcome of investigation.

From an ethical viewpoint it is interesting how the press reported the incident and raised unconnected issues e.g. an MP had been a computer teacher at a TAFE college. The mini case study showed two main ethical issues:

- The MPs son has access to his father’s Parliament House work computer and was able to install computer software. The aim of the software was to scan network for security vulnerabilities e.g. the network at parliament house. An ethical solution would be to ensure that users do no allow other people to use their computers;
- The accusation that IT staff had accidentally downloaded sensitive computer files upon another users computer. The ethical dilemma is if it happened, why? If the IT staff did download the material accidentally then it is an issue of professionalism, if they did with intention to cause harm it is an issue of unethical behaviour.

At the end of the day no criminal charges were placed and the matter was resolved. If some simple ethical guidelines had been applied the whole series of events would never have occurred in the first place.
Conclusions

As stated before in regards to the Auscert survey, computer crime is a problem within Australia and to resolve this some organisations are looking to hackers to solve their security problem. Is this Ethical?

Ethics is an extremely important component of Information Security, but the problem is that Information Security tends to just concentrate on internal processes of access and amendment rights. The introduction of deception techniques (Honeypots & Honeynets) to trap hackers can technically be effective and has been proven to work. However, from an ethical viewpoint should deception techniques be used to capture hackers?

References


Network Associates (2000) Cybercop Sting. URL:
http://www.nai.com/asp_set/products/tns/ccsting_intro

Spitzner, L. (2000a) To Build a Honeypot. URL: http://project.honeynet.org/papers/honeypot/


Spitzner, L (2000c) To Build a Honeynet, FIRST (Forum of Incident Response & Security Teams) Conference 2000, Chicago, USA.
Reflections on the Australian Computer Society Code of Ethics

S. L. Wheeler

School of Accounting and Information Systems
University of South Australia
Email: shirley.wheeler@unisa.edu.au

Abstract

As computer ethics play such an important role in global communication as well as the life of the computer professional and associated stakeholders, the ACS Code of Ethics is vital for guiding ethical norms and possibilities. In this paper, the Code is rearranged to fit ethical categories, as well as information systems stakeholder categories. Reflections involved in this process and some resulting suggestions for improvement are summarized.

Keywords: computer ethics codes; professional standards; information systems

Introduction

Contemporary ethical analysis and decision-making involve various tools, the main ones being:

- virtue (character orientated ethics);
- deontological (rules, duties, principles, means orientated) ethics;
- teleological (goals or ends orientated) ethics;
- stakeholders;
- contracts;
- normative and relative components (e.g. Hartman 1998, Mason, Mason & Culnan 1995).


Apart from acting ‘in good personal conscience’, and any other ethical conditioning that the Australian computer professional may have picked up along life’s learning pathway, the Australian Computer Society Code of Ethics (ACS) is perhaps the main ethical guidance resource available in times of professional ethical dilemma. This paper provides a preliminary analysis of the ACS Code of Ethics according to the main ingredients of ethical analysis. It was inspired by Rogerson, Weckert and Simpson’s mapping of the ACS Code of Ethics onto SSADM (Rogerson et al. 2000, p. 121).

The virtues identified by philosophers such as: Aristotle in Greece (Aristotle 325BC/1962); Confucius in China (Confucius ca500 B. C.); the Apostle Paul in Galatians 5 of the Holy Bible (1st Century AD); Bennett (1993) and Stephanie Dowrick (1997); vary considerably. Instead of using a specific virtue checklist, it may be more helpful to consider virtue clusters of similar characteristics. For example, virtue terms such as ‘honesty’, ‘reliability’, ‘trustworthiness’, and ‘respect
for others’ property’ do seem to have a lot in common, and can, for the sake of convenience, be clustered together to give a general idea of a particular set of virtues. Deontological and teleological guidelines can be ‘obligatory, or merely an aspiration’ (http://www.is.cityu.edu.hk/Research/Resources/ethics/ethics.htm; & www.isworld.org/Ethics/Professional Ethics). Nevertheless, codes of ethics are adopted by a community ‘because its members accept the adherence to these rules, including the restrictions that apply’ (Ibid). In effect, as a result of the professional experience gained, the codes encapsulate the norms of expected of a professional and the scope for variation.

**Computer Professionals’ Stakeholders**

As part of a comprehensive Multiview approach to Information Systems, an interdisciplinary professional field that relies heavily on computer technology (e.g. Mason et al. p. 66-67, Checkland & Holwell 1998, p. 62), Wood-Harper et al. (1999, p. 68) identified a comprehensive set of seven information systems stakeholder categories. These stakeholder categories are linked to an information systems developmental model in a hierarchical way (Avison & Wood-Harper 1986, cited in Avison et al. 1987, p. 199):

- Owner (e.g. the company owner, the intellectual property holder)
- Worldview (e.g. government and management assumptions, ethical code formulators)
- Actor (e.g. computer professionals, such as analysts, programmers, technicians)
- Transformation (e.g. inputs and outputs of the intended project changes, such as suppliers, new staff roles, deliverers)
- Client (e.g. members of another corporate department, retailers, users)
- Ethics (e.g. ethics officers, legal profession, educators)
- Environment (e.g. those living near the project; animal habitat protectors)

Different stakeholders can be included in the different sets according to the project definition. For example, educators can be owners of computer education material and courses in the corporate higher education sector, or educators could be in the role of interested lobbyists when there is an environmental danger, such as toxic toner powder use and dumping. Watson et al. (2000, p. 4) list ‘administrators’, ‘the business community’ and ‘colleagues in other disciplines’ as information systems (IS) stakeholders, and these can be subsumed under the appropriate main headings, such as: either ‘management worldview’ or ‘actors’; ‘clients’; and ‘clients’, respectively. The type of interest the stakeholder group has in the individual IS project and how wide the stakeholder net is cast, contribute to ascertaining their particular role in the stakeholder model at a particular time. There can be overlap in the model, with one stakeholder having a stake in several different stages and outcomes of the project. Mitroff and Linstone (1993) define a stakeholder as: ‘any individual, group, organization, or institution that can affect or be affected by an individual’s, group’s, organization’s, or institution’s policy or policies.’

**Australian Computer Society (ACS) Code of Ethics**

Given that the ACS Code of Ethics (www.isworld.org/ethics) is viewed as a norm for contracted computer professionals in Australia, the following table summarizes a
reflection on how this ACS code may be organised (loosely) under the headings of the seven groups of stakeholders. As well, there is an attempt to categorize the components into: virtue, deontological and/or teleological ethics, and assess whether the components are regulatory (enforced with penalties) or aspirational (ideals to be emulated). The ultimate aim of this exercise is to review the adequacy of the code from the perspective of a new format, and possibly to see whether there is some greater possibility of formalising some or all of the code of ethics into computer programs and professional practice.

**Table 1: Multiview Headings together with the Australian Computer Society (ACS) Code of Ethics**

<table>
<thead>
<tr>
<th>Multiview Headings</th>
<th>Philosophy behind Multiview</th>
<th>Deontological and teleological aspects of ACS Code of Ethics</th>
<th>Associated virtue ethics cluster examples from ACS Code of Ethics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Owner</strong> – the eventual system owner</td>
<td>Relates to integrity in relation to the highest goals of business leadership, etc. (respect for highest ownership conceivable and responsibility for all the stakeholders) In the ACS Code of Ethics, the items under this owner/professional integrity heading, as in all the other six stakeholder headings, seem to be largely aspirational in character, without any set punishments for breaches by ACS members.</td>
<td><strong>Deontological &amp; Teleological:</strong> A Requirement: members are required ‘to subscribe to a set of values and ideals which uphold and advance the honour, dignity and effectiveness of the profession of information technology’ 4.1. ‘uphold and advance the honour, dignity and effectiveness of the profession of information technology’ 4.1.c ‘strive to increase the competence and prestige of the profession’ 4.1.d ‘use special knowledge and skill for the advancement of human welfare’ 4.5.1 ‘I must endeavour to preserve continuity of information technology services and information flow in my care’</td>
<td><strong>Integrity, honour, dignity, professional effectiveness and survival, loyalty, wisdom, understanding, knowledge, sincerity, consideration for reputation in community</strong> 4.1.a ‘honest, forthright, impartial’, 4.1.b ‘loyally serve the community’ 4.1.c ‘strive to increase the competence and prestige of the profession’ 4.1.d ‘use special knowledge and skill for the advancement of human welfare’ 4.5.1 ‘I must endeavour to preserve continuity of information technology services and information flow in my care’</td>
</tr>
</tbody>
</table>
### Worldview – the assumptions of those with influence on the IT project, such as management personnel

<table>
<thead>
<tr>
<th>Knowledge and skill for the advancement of human welfare’</th>
<th>4.5.1 ‘I must endeavour to preserve continuity of information technology services and information flow in my care’</th>
<th>4.5.2 ‘I must endeavour to preserve the integrity and security of the information of others.’</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.6 ‘I must enhance the integrity of the IT profession’</td>
<td>4.10.8 ‘I must do what I can to ensure that the corporate actions of the Society are in accordance with this Code of Ethics.’</td>
<td>4 10.9 ‘I acknowledge my debt to the computing profession and in return must protect and promote professionalism in information technology.’</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Diplomacy discretion, politeness, deference</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.2 ‘I must place the interests of the community above those of personal and sectional interests.’</td>
</tr>
<tr>
<td>4 3.6 ‘I must enhance … the respect of (the IT professions’s) members for each other.’</td>
</tr>
<tr>
<td>4 3.2.4 ‘I must endeavour to understand, and give due regard to, the</td>
</tr>
</tbody>
</table>
| Client – the system’s beneficiary | Relates to respect for client’s property and wealth | 4.3.2 ‘I must work competently and diligently for my clients and employers’ 4.3.3 ‘I must be honest in my representation of skills, knowledge services and products.’ 4.6. More detail of the requirement for ‘competence’ is provided, which has some overlap with other headings 4.7. More detail of the application of ‘honesty’ is provided. 4.8.2 ‘I must consider and respect people’s privacy which might be affected by my work.’ 4.10.1 obtaining colleagues’ advice on competency where necessary. 4.10.2 ‘I must not knowingly engage in, or be associated with, dishonest or  

Honesty, competence, trustworthiness, reliability  
4.3.2 ‘I must work competently and diligently for my clients and employers’ 4.3.3 ‘I must be honest in my representation of skills, knowledge services and products.’ 4.6. More detail of the requirement for ‘competence’ is provided, which has some overlap with other headings 4.7. More detail of the application of ‘honesty’ is provided. 4.8.2 ‘I must consider and respect people’s privacy which might be affected by my work.’ 4.10.1 obtaining colleagues’ advice on competency where necessary. |
| **Actor** – the individual(s) involved in the system, such as IT professionals | Relates to staff culture and stakeholder relationships (respect for all the actors involved in the interactions) | 4.3.4 ‘I must strive to enhance the quality of life of those affected by my work.’  
4.3.6 ‘I must enhance … the respect of … members for each other.’  
4.5.3 ‘I must respect the proprietary nature of the information of others.’  
4.8.1 ‘I must protect and promote the health and safety of those affected by my work’  
4.8.2 ‘I must consider and respect people’s privacy which might be affected by my work.’  
4.8.5 ‘I must attempt to increase the feelings of personal satisfaction, competence, and control of those affected by my work’  
4.10.1 ‘I must respect, and seek when necessary, the professional opinions of colleagues in their areas of competence.’  
4.10.3 ‘I must not attempt to enhance my reputation at the expense of another’s reputation.’  
4.10.4 ‘I must cooperate in advancing information processing by | 4.10.2 ‘I must not knowingly engage in, or be associated with, dishonest or fraudulent practices.’  

**Respectfulness, congeniality, faithfulness, conviviality, pleasantness helpfulness**  

4.3.4 ‘I must strive to enhance the quality of life of those affected by my work.’  
4.3.6 ‘I must enhance … the respect of … members for each other.’  
4.5.3 ‘I must respect the proprietary nature of the information of others.’  
4.8.1 ‘I must protect and promote the health and safety of those affected by my work’  
4.8.2 ‘I must consider and respect people’s privacy which might be affected by my work.’  
4.8.5 ‘I must attempt to increase the feelings of personal satisfaction, competence, and control of those affected by my work’  
4.10.1 ‘I must respect, and seek when necessary, the professional opinions of colleagues in their areas of competence.’  
4.10.3 ‘I must not attempt to enhance my
| **Transformation** – intention of the project | **Relates to business strategies and respect towards stakeholders in a situation of change and possibly some stress, particularly those who may seem obstructive (transformational intent on improvement, rather than devaluation of unsatisfactory stakeholders)** | **4.3.5 ‘I must enhance my own professional development, and that of my colleagues, employees and students.’**
4.5.3 ‘I must respect the proprietary nature of the information of others.’
4.8.6 ‘I must not require, or attempt to influence, any person to take any action which would involve a breach of the Code of Ethics.’
4.9.1-3 ‘Professional Development’ involves self-discipline and resourcefulness to advance from one’s previous mindset.
4.10.5 ‘I must distance myself professionally from someone whose membership of the Society has been terminated because of unethical behaviour or unsatisfactory conduct.’ | **Self-restraint, self-discipline, courage, patience, resourcefulness, caring**
4.3.5 ‘I must enhance my own professional development, and that of my colleagues, employees and students.’
4.5.3 ‘I must respect the proprietary nature of the information of others.’
4.8.6 ‘I must not require, or attempt to influence, any person to take any action which would involve a breach of the Code of Ethics.’
4.9. ‘Professional Development’ involves self-discipline and resourcefulness to advance from one’s previous mindset.
4.10.5 ‘I must distance myself professionally from someone whose...’ |
| **Ethics** – which involves stakeholders in evaluating ethical considerations and redressing injustices | Relates to the evaluation of business practice, such as in annual reports and internal reporting procedures together with appropriate means and procedures for the redress of unethical behaviour (evaluation of ethical practice) | 4.5.5 ‘I must advise my client or employer of any potential conflicts of interest between my assignment and legal or other accepted community requirements.’ 4.5.6 ‘I must advise my clients and employers as soon as possible of any conscientious objections which face me in connection with my work.’ 4.8.3 ‘I must respect my employees and refrain from treating them unfairly’ 4.10.6 ‘I must take appropriate action if I discover a member, or a person who could potentially be a member, of the society engaging in unethical behaviour.’ 4.10.7 ‘I must seek advice from the Society when faced with an ethical dilemma I am unable to resolve by myself.’ | **Fairness, impartiality, justice, mercy, harmony, decisiveness, courage, strength of character** 4.5.5 ‘I must advise my client or employer of any potential conflicts of interest between my assignment and legal or other accepted community requirements.’ 4.5.6 ‘I must advise my clients and employers as soon as possible of any conscientious objections which face me in connection with my work.’ 4.8.3 ‘I must respect my employees and refrain from treating them unfairly’ 4.10.6 ‘I must take appropriate action if I discover a member, or a person who could potentially be a member, of the society engaging in unethical behaviour.’ 4.10.7 ‘I must seek advice from the Society when faced with an ethical dilemma I am unable to resolve by myself.’ |
Some Observations

There is some overlap in categories, both in the ACS Code of Ethics and in the ethical theory application. For example, there is a lot written on the areas of ‘competence’ and ‘honesty’ in the ACS Code of Ethics, and when the material is categorised together, the overlap is more clearly visible. This could be more efficiently streamlined. In relation to the ethical theory, sometimes the listed teleological goals are the achievement of a virtue, such as honesty or competence, and the form of the related Code of Ethics statement is deontological (e.g. ‘I must be honest’). Thus, at times, there is a repetition of the same statements under the deontological, teleological and virtue cluster headings. Perhaps this could be a little better clarified in future, by some division into goal, means (deontological) and end indicator of goal (teleological) achievement. Given the prevalence of triple bottom line reporting requirements (Gray et al. 1996), the ACS has no definite mention of the environment, which may reflect the positivist domination of the IT profession (Allen & Ellis 2000, Jayaratna 1994), but it ill equips the modern computer professional for including environmental perspectives and dealing with environmental ethical dilemmas. There is not much in the ACS Code of Ethics regarding work contracts, yet these have a very strong effect on the way that stakeholders interact. For example, technicians can reflect their work contract in avoiding any involvement in ethics, and contractors can neglect to include particular stakeholders (such as those with environmental concerns) or to suggest better ways of doing things, as this possibility is not specified in their work contracts. Perhaps there could be more on the design of work contracts to better include wider stakeholder perspectives, as well as dispute resolution processes, in future ACS Codes of Ethics.

References


The Analects of Confucius (ca 500 B. C.),


Holy Bible, King James version.


## Authors Index

<table>
<thead>
<tr>
<th>Author</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ÄHLFELDT</td>
<td>6</td>
</tr>
<tr>
<td>BURMEISTER</td>
<td>51, 106, 118</td>
</tr>
<tr>
<td>BRANKOVIC</td>
<td>39</td>
</tr>
<tr>
<td>CLARKE</td>
<td>16</td>
</tr>
<tr>
<td>FURNELL</td>
<td>22</td>
</tr>
<tr>
<td>GIBBS</td>
<td>30</td>
</tr>
<tr>
<td>GIGGINS</td>
<td>39</td>
</tr>
<tr>
<td>HARDY</td>
<td>51</td>
</tr>
<tr>
<td>HUTCHINSON D</td>
<td>57</td>
</tr>
<tr>
<td>HUTCHINSON W</td>
<td>139</td>
</tr>
<tr>
<td>KING-SIEM</td>
<td>68</td>
</tr>
<tr>
<td>LEITCH</td>
<td>73</td>
</tr>
<tr>
<td>MORRISON</td>
<td>68</td>
</tr>
<tr>
<td>NEVILLE</td>
<td>118</td>
</tr>
<tr>
<td>PHYO</td>
<td>22</td>
</tr>
<tr>
<td>ROBERTS S</td>
<td>106</td>
</tr>
<tr>
<td>ROBERTS P</td>
<td>80, 88</td>
</tr>
<tr>
<td>SANDY</td>
<td>96</td>
</tr>
<tr>
<td>SCOTT</td>
<td>106</td>
</tr>
<tr>
<td>SIMPSON</td>
<td>118</td>
</tr>
<tr>
<td>SPARROW</td>
<td>128</td>
</tr>
<tr>
<td>VALLI</td>
<td>130</td>
</tr>
<tr>
<td>WARREN</td>
<td>57, 73, 139</td>
</tr>
<tr>
<td>WEBBER</td>
<td>88</td>
</tr>
</tbody>
</table>