ETHICS AND THE INTERNET

2 Key Ethical Concepts for the Internet and for Ethical Codes of Computer Professionals
PORFIRIO BARROSO ASENJO

6 Law, Ethics and the Internet: Finding Solid Ground in Virtual Spaces
BRIAN M O'CONNELL

12 Privacy and the Internet
SEUMAS MILLER

16 Australian Approaches to Internet Content Regulation
JAMES M HOGAN, PETER CJ JAMES

24 Copyright in Shareware Programs Distributed on the Internet
CRISTINA CIFUENTES, ANNE FITZGERALD

31 Internet Ethics' Bibliography
PORFIRIO BARROSO ASENJO

SPECIAL FEATURES

1 Guest Editorial

30 Call for Papers — Software Quality Conference

35 Book Reviews

Published for Australian Computer Society Incorporated
Print Post Approved PP255003/01660
The Australian Computer Journal is an official publication of the Australian Computer Society Incorporated.

CONTRIBUTIONS
All material for publication should be sent to:
Mr David Wilson
School of Computing Sciences
University of Technology, Sydney
PO Box 123, Broadway NSW 2007, Australia

Prospective authors may wish to consult manuscript preparation guidelines published in the February 1995 issue. The paragraphs below briefly summarise the essential details.

Types of Material: Four regular categories of material are published: Papers, Short Communications, Letters to the Editor and Book Reviews.

Generally speaking, a paper will discuss significant new results of computing research and development, or provide a comprehensive summary of existing computing knowledge with the aim of broadening the outlook of Journal readers, or describe important computing experience or insight.

Short Communications are concise discussions of computing research or application. A letter to the Editor will briefly comment on material previously appearing in the Journal, or discuss a computing topic of current interest. The term 'computing' is interpreted broadly to include descriptions of computer hardware and software, and major computer applications such as information systems, expert systems, computer networks and office automation.

Refereeing: Papers and Short Communications are accepted if recommended by anonymous referees. Letters are published at the discretion of the Editor, and Book Reviews are written at the Editor’s invitation upon receipt of review copies of published books. All accepted contributions may be subject to minor modifications to ensure uniformity of style. Referees may suggest major revisions to be performed by the author.

Proofs and Reprints: Page proofs of Papers and Short Communications are sent to the authors for correction prior to publication. Fifty copies of reprints will be supplied to authors without charge. Reprints of individual papers may be purchased from Associated Business Publications Pty Ltd, PO Box 267, Umina, NSW 2257. Microfilm reprints are available from University Microfilms International, Ann Arbor/London.

Format: Papers, Short Communications and Book Reviews should be typed in double spacing on A4 size paper, with 2.5 cm margins on all four sides. The original, plus two clear bond paper copies, should be submitted. References should be cited in standard journal form, and generally diagrams should be ink drawn on tracing paper or board with stencil or Letraset lettering.

Ideally, a hard copy, a 3½” Apple disk in QuarkXpress or PageMaker, alternatively Microsoft Word is required. Straight text papers may be submitted in ASCII on 3½” disk.

Papers and Short Communications should have a brief Abstract, Key word list and CR categories on the leading page, with authors’ affiliation as a footnote. The authors of an accepted paper will be asked to supply a brief biographical note for publication with the paper.

Copyright © 1997 Australian Computer Society Inc.

Production Management:
Associated Business Publications Pty Ltd (ACN 002 328 154), PO Box 267, Umina 2257.
Telephone (043) 41 3628, Fax (043) 42 5624.
All advertising enquiries should be referred to the above address.

Proofs and Reprints: Page proofs of Papers and Short Communications should be returned to the above address.

Referees may suggest major revisions to be performed by the author. Acceptance of contributions may be subject to minor modifications to ensure uniformity of style. Referees may suggest major revisions to be performed by the author.

Proofs and Reprints: Page proofs of Papers and Short Communications are sent to the authors for correction prior to publication. Fifty copies of reprints will be supplied to authors without charge. Reprints of individual papers may be purchased from Associated Business Publications Pty Ltd, PO Box 267, Umina, NSW 2257. Microfilm reprints are available from University Microfilms International, Ann Arbor/London.

Format: Papers, Short Communications and Book Reviews should be typed in double spacing on A4 size paper, with 2.5 cm margins on all four sides. The original, plus two clear bond paper copies, should be submitted. References should be cited in standard journal form, and generally diagrams should be ink drawn on tracing paper or board with stencil or Letraset lettering.

Ideally, a hard copy, a 3½” Apple disk in QuarkXpress or PageMaker, alternatively Microsoft Word is required. Straight text papers may be submitted in ASCII on 3½” disk.

Papers and Short Communications should have a brief Abstract, Key word list and CR categories on the leading page, with authors’ affiliation as a footnote. The authors of an accepted paper will be asked to supply a brief biographical note for publication with the paper.

Copyright © 1997 Australian Computer Society Inc.

Production Management:
Associated Business Publications Pty Ltd (ACN 002 328 154), PO Box 267, Umina 2257.
Telephone (043) 41 3628, Fax (043) 42 5624.

All advertising enquiries should be referred to the above address.

Proofs and Reprints: Page proofs of Papers and Short Communications should be returned to the above address.

Referees may suggest major revisions to be performed by the author. Acceptance of contributions may be subject to minor modifications to ensure uniformity of style. Referees may suggest major revisions to be performed by the author.
The May 1990 issue of this journal was devoted to social aspects of computing. In the intervening years the study of computer ethics, one component of these social aspects, has flourished, if not so much in Australia, certainly in the United States and Europe. There are now numerous conferences and centres devoted to this study; a study which focuses on how people ought to behave with respect to computer technology. The ethical problems which are spawned by the use of computer technology are not new. Ethics has been studied systematically at least from the time of the ancient Greeks, and the examination of ethical issues in computing are just part of this tradition. What is significant in this examination is that the development and use of computers has raised old questions in interestingly new and different ways. This has become even more evident in the last few years as the Internet has grown rapidly. Various old moral problems have become more urgent. The emergence of freedom of speech and censorship as an important topic in computer ethics is largely a result of the Internet expansion. Electronic publishing, and the digital storage and transfer of information facilitated by the Internet, has lead to growing concern about intellectual property. The ever increasing amount of information accessible by and carried on the Internet has also heightened worries about privacy. While these are currently perhaps the most central ethical concerns on the Internet, and are those which will receive most attention in this special issue, they are by no means the only ones. There is frequent discussion on the Internet about the morality of “spamming” and “flaming”. More important perhaps is the deception which is so easy to perpetrate. The best known example of this is probably the male New York psychiatrist who masqueraded as a physically disabled female neuropsychologist, in order, supposedly, to help women. The problem of dangerous information, for example instructions for the manufacture of bombs, being available on the Internet is another often debated topic, along with questions of accuracy and reliability of information, and Internet access. Less often discussed is the waging of war over communications networks, and the possibility of cultural domination by the more powerful nations and groups. This list of ethical issues is not complete. It is merely intended to show the range of moral problems related to the Internet.

The study of ethics means many different things to many different people, and ethical issues can be examined from a number of different perspectives. These perspectives include philosophical, legal, technical, psychological, and sociological. A complete examination involves all, but most discussions are limited to only one or two. The main reasons for this are probably first, that most people are competent in only one discipline, and second, that in order to achieve depth in a journal article-length discussion there must be a sharp focus. These different perspectives can be illustrated by a consideration of privacy. Miller’s article is a philosophical examination of some of the basic ideas underlying privacy; what it is and why it is desirable (if it is). A legal discussion would focus on what the law says about privacy, and might examine cases and interpretations of the law. From a technical point of view, the interesting questions revolve around how to protect private information on the Internet, and one central concern would be encryption. A psychologist’s main interest would be in the effects of privacy, or its lack, on individuals, while the sociologist would be more concerned with the social effects of privacy. These perspectives are related. Legal and philosophical discussions of privacy on the Internet take place within the parameters of what it is technically possible to do. A significant part, though not all, of philosophical examinations of ethical questions concerns consequences of actions, and this is where much of the importance of psychology and sociology lies.

Why does any of this matter to the computer professional? It matters for two reasons. As professionals we are involved in day-to-day decisions about what we ought to do, and also in policy making. A rational and thoughtful discussion of moral issues can aid in both of these. Hopefully, the papers here will contribute to this and to one goal of the ACS, which is to “use [our] special knowledge and skill for the advancement of human welfare” (Code of Ethics, 4.1) and to “enhance the quality of life of those affected by [our] work” (Code of Ethics, 4.3.4).

The following papers, from three countries, reflect some of the main debates and problems in current Internet ethics. The first, by Porfirio Barroso Asenjo, is a study of how various professional codes of ethics in a number of countries support some key concepts in Internet ethics. In the second, Brian O’Connell examines the concept of the Internet as a community, in order to find a basis for a discussion of the ethical and legal questions. Both of these contributions are concerned with some important general issues, while the next three papers concentrate on specific topics. As it has already been noted, Seumas Miller examines the notion of privacy and applies this to some privacy questions on the Internet. The fourth paper, by James Hogan and Peter James, examines censorship, particularly in the Australian context. Copyright is the last topic, and Cristina Cifuentes and Anne Fitzgerald discuss a recent shareware case. This special issue concludes with a comprehensive bibliography on Internet ethics, compiled by Porfirio Barroso Asenjo.

I thank the following people for acting as referees for this special issue:

Andrew Alexandra
Bob Eddy
Craig McDonald
Paula Roberts
Michael Whitelaw

Roger Clarke
Jennifer Goddard
Ann Moffatt
Elizabeth Sonnenberg

Joan Cooper
Frank James
Robert Neely
Max Staples

John Weckert,
Charles Sturt University
Key Ethical Concepts for the Internet and for Ethical Codes of Computer Professionals

Porfirio Barroso Asenjo
Complutense University, Madrid and Pontificial University, Salamanca, Spain

In this research, five hundred letters were sent to computer science professionals to ask for all of the ethical codes of their organisations and enterprises. Fifteen different codes were received. A computerised analysis of the contents of each code was undertaken. Forty ethical principles or rules were identified, and these were listed in decreasing order of quantitative appearance in the codes. Those ethical principles appearing at least 17 times (nearly half of the maximum number of appearances) were compared to four key ethical concepts identified by Mason (1986) as central to the future success of computing. The results of this research and another survey by Berleur and Brunnstein (1996) show that codes of ethics of IS professionals do treat as very important the four ethical issues singled out by Mason. Arguments by Platt and Morrison (1995) indicate that these results provide positive evidence that IS professionals are addressing social and ethical concerns that will advance and support the Internet and future global computer networks.

Keywords: Access, Accuracy, Codes of Ethics, Computer Ethics, Computer Science, Confidentiality, Intellectual Property, Internet Privacy

INTRODUCTION

In 1986, Richard Mason published an influential article in *MIS Quarterly* entitled ‘Four Ethical Issues of the Information Age’ (Mason, 1986). In that article, Mason identified four topics as key ethical issues that are central to applications of information technology. These topics, which he summarised with the acronym PAPA, are ‘privacy’, ‘accuracy’, ‘property’, and ‘accessibility’.

Richard G Platt and Bruce Morrison (1995) have argued that successful handling of these four ethical issues is crucial to the future success of the Internet and its successors:

“We are now at a place in the life of the Internet where it is make or break. While the potential pitfalls are many, they are as critical as they are simply because the potential of the NII [National Information Infrastructure] is so great. Ignoring issues of privacy, accuracy, intellectual property, and access, will surely kill that potential. With the volume of knowledge available to humanity, the loss of this resource would have a devastating effect on the quality of human life.

If privacy becomes a joke in cyberspace, then the medium will be shunned by both providers and consumers as being too risky to entrust with personal or proprietary data. In the same vein, if accuracy cannot be trusted on-line, the only solution would be, regrettably, to reject this mode of communication as being too risky. Universally free information, while superficially attractive, would grind to a halt most sharing of new and old knowledge. This is obviously not an option. And while none of these can be ignored, probably the greatest opportunity for gain, and the most dangerous if ignored, is the assurance that all people have access to information. For this is increasingly becoming the most valuable commodity in our society. And as we seem to be becoming more divided by education, economics, and understanding every year, an inequitable division of this treasure is a formula for disaster.

While these all have the flavour of doom, they are merely warnings. The only real danger is ignorance of the implications. For the person who encounters these situations and evaluates them in an ethical manner can handle them effectively. Only with ignorance and neglect comes disaster” (Platt and Morrison, 1995).

If Platt and Morrison are correct that PAPA are crucial to the future success of the Internet and its successors, an interesting and important question can be raised: Do the codes of ethics of professional computer societies encourage or require respect for privacy, accuracy, property and accessibility?

Two recent surveys of codes of ethics among professional computing societies shed light on this important question. One is a study of 30 codes of ethics presented by Jacques Berleur and Klaus Brunnstein in their book *Ethics of Computing: Codes, Spaces for Discussion and Laws* (Berleur and Brunnstein, 1996). And the other survey is a study that the
present author conducted in 1994 and 1995 of 15 codes of ethics of professional organisations or companies in the field of computing.

**Results of the Berleur and Brunstein Survey**

The Berleur and Brunstein survey is the result of an IFIP (International Federation for Information Processing) project that included analyses of the codes of ethics of 30 societies of computing professionals from a number of countries in Europe, America, Africa and Asia. Berleur and Brunstein found that five main topics are developed in nearly all the codes. These include:

- Respectful general attitude
- Personal (/institutional) qualities, such as conscientiousness, honesty and positive attitude, competence and efficiency
- Promotion of information privacy and data integrity
- Production and flow of information
- Attitude towards regulations

Under "Promotion of information privacy and data integrity", Berleur and Brunstein include (among other topics) "privacy in general", "confidentiality", "respect for property", and "accuracy". Under "Production and flow of information", they include flow of information "to the society (or public)". The Berleur and Brunstein analysis shows that a majority of codes of ethics in their survey encourage or require respect for privacy, accuracy, property and accessibility. The Berleur and Brunstein research, then, does support the view that codes of ethics of professional societies encourage PAPA.

**Description of the Present Research**

Another survey, conducted by the present author in 1994 and 1995, yielded similar results regarding codes of ethics and support of PAPA. In this survey, 500 key people around the world in professional informatics associations or heads of departments of informatics in governments, international organisations and corporations were contacted and asked to provide copies of any codes of informatics ethics that their organisations had. 15 codes of ethics (excluding duplicates) from seven different countries were received. Most of these were codes from professional associations such as the Association for Computing Machinery; the British Computer Society; the Australian Computer Society; the Information and Computing Service Association (Ireland); the Data Processing Management Association (USA); as well as codes from the IBM Corporation; the Center for Informatics, Telematics and Related Media (Spain); and holders of the Certificate in Data Processing (USA).

The content of each of the codes was analysed, yielding a total of forty ethical principles. Occurrences of these were entered into a database using the software DBASE-IV, creating 515 records. The frequency of occurrence of each of the principles was then determined by computer analysis. The frequency of occurrence was considered to be important, because it indicates the different interpretations of the ethical fundamentals, as well as the diversity of comprehension and extension of the ethical norms and guidelines presented in the codes.

Once the frequency of occurrence of each principle was determined, the principles were arranged in decreasing order of frequency.

**Results of the Analysis**

Frequencies ranged from a maximum of 36 occurrences of an ethical principle in the codes of ethics to a minimum of two occurrences. Ethical principles with at least 17 occurrences (nearly half of the maximum or more) were the following:

- **36 Occurrences:** Principle 1 — The IS professional should respect the confidentiality of information with which he/she deals.
- **34 Occurrences:** Principle 2 — The IS professional should behave in a professionally responsible way.
- **33 Occurrences:** Principle 3 — The IS professional should be loyal to his company, his clients and the general public.
- **26 Occurrences:** Principle 4 — The IS professional should act with dignity, honesty and integrity.
- **25 Occurrences:** Principle 5 — The IS professional should serve above all the common good and the public interest. (Put social benefits above personal benefits.)
- **23 Occurrences:** Principle 6 — The IS professional should have quality academic preparation and remain well prepared by means of continuing education.
- **21 Occurrences:** Principle 8 — The IS professional should accept no bribes, including enticements in the form of gifts and entertainment.
- **20 Occurrences:** Principle 10 — The IS professional should transmit data with accuracy.
- **19 Occurrences:** Principle 12 — The IS professional should use fairness and equity in dealing with others.
- **18 Occurrences:** Principle 14 — The IS professional should provide services based upon professional knowledge, skill and ability.
- **17 Occurrences:** Principle 15 — The IS professional should respect and protect intellectual property by obeying copyrights, mentioning sources, making appropriate citations and references.
Survey Results Regarding Codes of Ethics and PAPA
The four key ethical concepts identified by Mason and abbreviated as “PAPA” are “privacy”, “accuracy”, “property” and “accessibility”. As indicated above, Platt and Morrison argue persuasively that these four issues are crucial to the continuing success of the Internet and its successor, the NII (National Information Infrastructure). Indeed, Platt and Morrison actually mean the “GII” or “Global Information Infrastructure”.

The results of the latest survey clearly show that the codes of ethics of the representative organisations do indeed include PAPA among the important ethics principles supported. The PAPA principles (or closely related ones) occurred at least 17 times in the various ethical codes analysed. In particular:

36 Occurrences: Principle 1 — The IS professional should respect the confidentiality of information with which he/she deals.

21 Occurrences: Principle 9 — The IS professional should uphold and exercise the right to provide and receive information.

20 Occurrences: Principle 10 — The IS professional should transmit data with accuracy.

Principle 11 — The IS professional must avoid invasions of privacy.

19 Occurrences: Principle 12 — The IS professional should use fairness and equity in dealing with others.

17 Occurrences: Principle 15 — The IS professional should respect and protect intellectual property by obeying copyrights, mentioning sources, making appropriate citations and references.

Privacy — Principle 1 concerns “confidentiality” and Principle 11 concerns “invasions of privacy”. These two concepts are closely related. If someone keeps personal information secret, it is said to be private information. If private information is shared with others, with the understanding that those others will share it only with those who have a right to it, the information is said to be confidential. Principles 1 and 11 together require that IS professionals treat private and confidential information with respect by not sharing it with others who have no right to it.

We read in the Code of Conduct for the Information and Computing Services Association (Ireland), “to impress upon employees and periodically remind them of the confidential nature of the Client’s material and information”. In the DPMA Code of Ethics (USA), the IS professional has the obligation, and must pledge not, to use the data available to him or her through professional secrecy. “I shall not use knowledge of a confidential nature to further my personal interest, nor shall I violate the privacy and confidentiality of information entrusted to me or to which I may gain access”. The Code of Ethics, Conduct and Good Practice for Holders of the Certificate in Data Processing (USA) includes, under professional secrecy of the IS professional, any information to which he or she has access through working with computers. From the ACM (Association for Computing Machinery) Code of Professional Conduct, we take the following quotation: “An ACM member shall not use any confidential information from any employer or client, past or present, without prior permission”.

Accuracy — Principle 10 requires that IS professionals safeguard the accuracy of information that is in their care. Correct information should be secured in the first place and it should be guarded and made secure from inappropriate alteration.

We define accuracy as faithfulness and preciseness in the transmission of data. Everyday people make assumptions about the information they are given. If the newspaper makes a certain claim, then most people are inclined to believe it. If they were knowledgeable enough to spot the falsehood, they would not be likely to read it in the first place. These assumptions are necessary to normal societal function. Given the complexity of modern life, if someone has extensive first-hand knowledge of one field, they are considered expert in that field. With the hundreds of thousands of areas of human knowledge, people most often have to trust information to a certain extent. In cyberspace this tendency to believe, probably because of the underlying complexity of the technology, is even more pronounced and even less justified (Neumann, 1992).

Property — Principle 15 instructs IS professionals to respect the personal property of others and to give appropriate references and citations to assure that the intellectual property of others is acknowledged when it is used in research or writing. Copyrights and other legal protections of property should be appropriately obeyed.

Traditional protections of intellectual property, such as patents and copyrights, are based primarily on the concept that encouraging the “discoverer” to share her/his knowledge with the rest of the “group” is a greater social benefit than simply “taking” it.

One of the most complex ethical issues in connection with ethics on the Internet is how to preserve and maintain an author’s intellectual property rights over his creation when one has access to it through the Internet. The IS professional should avoid copying programs, data bases, files, information and so on, which is intellectual property that doesn’t belong to him/her in order to avoid computer crimes that could be prosecuted by law.

Access — Principle 9 and Principle 12 together require that a person’s right to have information be respected and that this right be fairly and equally defended. As more and more human activities enter cyberspace — employment, business, education, medical services, entertainment — the gap between the rich and the poor will grow, unless access to computing, and especially to the Internet, is available to everyone rich and poor alike.

CONCLUDING REMARKS
The present survey of 15 codes of ethics from information organisations in seven countries confirms that privacy, accuracy, property and access (Mason’s key PAPA issues, 1986)
are all treated as very important by such organisations. The IFIP survey by Berleur and Brunstein (1996) yields a similar result. Platt and Morrison (1995) argue persuasively that appropriate concern for PAPA is crucial to the future success of the Internet and its successors. Since codes of ethics of professional organisations indicate which ethical issues those organisations take seriously, the results of these two surveys provide useful positive evidence that IS professionals are addressing social and ethical concerns that will advance and support the Internet and future global computer networks.

REFERENCES


BIOGRAPHICAL NOTES
Porfírio Barroso is Doctor of Philosophy and Doctor of Psychology and Bachelor of English Philology. Professor of the Complutense University of Madrid and of the Pontifical University of Salamanca, Spain.
1 INTRODUCTION

This paper is concerned with preliminary considerations for the development of ethical and legal principles applicable to the Internet. That laws will be written about this medium is inevitable. The acceptance and use of this technology has progressed to an extent that legislation such as the United States' Computer Decency Act of 1996 has already been enacted. That the Act is currently blocked in the courts demonstrates that litigation will be an additional source of rulings involving such issues as digital property, expression and privacy.

Once created, enforcement of these laws will not be a simple matter. The Internet operates within a global environment and what is decided in one country may not necessarily comport with the legalities of another. Uniformity of law and reciprocity of enforcement are not the only issues. In addition to possessing the potential of generating numerous international conflicts of law, it has been theorised that networked systems have their own ability to create and enforce rules of conduct (Branscomb, 1993).

The Internet currently presents legislators, judges and regulators with a complex set of problems. In terms of newness, this medium poses serious difficulties for the imposition of normal legal protocols. Traditionally, Anglo-American jurisprudence and to different extents, those of other origins are built upon the notion of precedent. This system relies upon the existence of prior decisions from which courts can identify 'rules' which then serve as solutions to the issue at hand (Benditt, 1987). The newness of the Internet and its dynamics hold obvious challenges to the application of precedent. Without clear historical precursors, lawmakers will either be compelled to create totally new law or will need to understand something about the dynamics of the Internet in order to devise effective analogies.

A related problem is raised by the question of jurisdiction. The Internet is a borderless operation in which information originating on one side of the globe can reach the other in a matter of seconds. Implementing effective national legal controls is immediately rendered problematic by the swiftness of transactions as well as by the ubiquity of the networks themselves (Harasim, 1993). Moreover, the rationale and intelligibility of each nation's regulations will certainly be a factor in the decision of other countries to afford reciprocal recognition of judgments and laws.

These dilemmas are but a few examples of the seemingly endless and diverse practical challenges which will present themselves to the courts and legislatures of the world. A legal response can come in two general forms. First, each issue can be addressed separately and serially. Such an approach is certainly not unthinkable and might well be imagined as the natural reaction of jurists and legislators who, being generally unfamiliar with the specifics of computers and related technology, are hesitant to adopt anything but a case-by-case treatment. Although understandable, this path could have the unfortunate consequence of creating a patchwork of laws and
rulings which if not in obvious conflict, may be too specific to the situation or technology at issue to provide any precedential guidance or any rationale to encourage recognition by other jurisdictions.

An alternative to the serial approach, and what is advocated in this paper, is a broader consideration of the human interactions which occur in virtual communications. This method accentuates the personal experiences, expectations and attitudes of the actual users. In conventional legal theory, it finds a counterpart in the observations of Ronald Dworkin (1986) that law must reflect an integrity and must be seen as coherent. To Dworkin, the concepts which exhibit these features are revealed in the social practices of the community, specifically those behaviours and world views which fuse its members to each other. This complex interplay of duties and obligations has been traditionally ignored by philosophers and legal theorists, who have more often emphasised law's transcendent reliance upon the more concrete models of "fair play" and social contract. Dworkin's theory provides a more abstract and, hence, more universally applicable vision of how accepted standards of conduct translate into laws which are regarded as just, fair and coherent.

The location of just law within community practices accomplishes several important practical legal goals. It shifts the emphasis of study from discernment of purely technological questions to the more familiar realm of human attitudes and behavior. A consequence is that both legislatures and courts may be less intimidated by issues which it may have heretofore felt no affinity or expertise. Most significantly, the focus upon interpersonal and community aspects divests rulings and legislation of the narrowness which is a hallmark of judgments based only upon technological functioning. Instead, the focus on shared human aspects promises to confer a universality and coherence which can enhance both precedential value and acceptance across geographic borders. In order to arrive at laws which will provide such results, jurists will need to examine the values which are manifested in the 'virtual community.'

2 ETHICS, LEGAL PRINCIPLES AND COMMUNITY
Ethics simply, but concisely defined, deals with what things are sought or avoided (Bok, 1979). It identifies what choices and behaviours may be considered to be of value. In traditional legal scholarship, ethics has been recognised as a foundation for the more specific and regulatory endeavour of law. If law can be viewed as a social system which accommodates itself to the community in which it exists (Post, 1995), then ethics provides the raw material in terms of the general values exhibited within the society. In Dworkin's community-focused jurisprudence, ethical determinations can be considered "pre-legal" in character, comprising elemental and abstract principles through which specific legal rights or injunctions are crafted.

Legal principles are unlike legal rules in that they do not represent the all-or-nothing determinations which we expect from statutes or the judgements of cases in controversy (Dworkin, 1979). Principles do not necessitate particular decisions, but form propositions which often argue for certain outcomes and thus become the motivating forces behind specific judgments. Legal principles exist before a case comes to trial or an issue is voted on by the legislature.

Before proceeding to consider specific ethical issues within the Internet, the nature of the landscape itself deserves some comment. Several years ago, the notion that a machine-centred phenomenon could be considered to have a dynamic ethical character would raise immediate questions. This is because ethical consideration of technology has traditionally focused on the instrumental nature of the subject.

Certainly, writings about technological determinism and related fields have addressed technology as an impetus of change (Heilbroner, 1994), but they are more accurately applications of a broader philosophical consideration. Ethical analyses on the other hand, have focused primarily upon how a technology is to be employed within a greater social arena. Medical ethicist, Eric Cassell (1993) summarises this approach when he states that "technology is not the problem; it is the relationship to it of those who employ it that is problematic."

Rather than functioning simply as a tool within the conventional framework of society, the Internet transcends instrumentalist definition. Instead, it presents ethical characteristics which are strikingly similar to those residing within more traditional communities. This is most apparent in the interactive nature of the medium.

Within the last decade, computing has undergone a massive transformation in how it is used and perceived by society. Some twenty-five years ago, a popular journal described computers as devices through which "man achieves the power to master information on a scale that profoundly influences the course of science, business government — even the arts" (White, 1970). While conventional data processing remains a typical function of digital technology, its pre-eminence has been eclipsed by what is broadly termed "computer-mediated communication" (CMC).

There are many forms of CMC. Electronic mail (email) is perhaps the most common. A variation, known as "listservs" allows messaging to numerous users who subscribe to share common interests. Similar activity occurs in Usenet newsgroups where messages are posted and responded to in a bulletin board format. More recently, the World-Wide Web has developed as a platform for a tremendous variety of graphical and textual presentations with site creators ranging from corporations to private individuals.

While email, Usenet and most web sites are available for access at any time and do not require the instantaneous presence of recipients, more immediate methods of communication are available within the Internet. These include the Internet Relay Chat (IRC) where messages are transmitted live, line-by-line. In addition, multi-user domains (MUDS) offer textual (and more recently, graphical) interfaces in
which users navigate their way through environments filled with objects and places of the participants’ own creation.

This brief catalog of interactive resources is not intended to be exhaustive. The modes of interaction have changed frequently and will likely do so well into the future. What is important within this context is the overwhelming popularity that CMC has achieved among a diverse group of people within a short period of time. This has not primarily been accomplished by the hardware features of the computer, but by a plasticity by which networked communications have allowed users to build their own environments.

The findings of the behavioural sciences support this phenomenon. While initially hypothesised to be an inhibitor of socialisation and a means of alienation (Sproull, Kiesler and Zubrow, 1984), investigators have found little to support claims of CMC-induced “deindividuation” (Matheson and Zanna, 1988). Rather, there is much evidence to suggest that networked communication encourages individual expression (Smilowitz, Compton and Flint, 1988) and reduces some forms of debilitating dominance patterns experienced in ‘analog’ society (Hesse, Werner and Altman, 1988).

Networked communication has been identified to take place in a social milieu which is complete with its own norms and rules (Newby, 1993). Anecdotal information abounds concerning the creation of long-term friendships, close-knit support groups, and means by which individuals maintain social contacts (Harasim, 1993; Rheingold, 1993; Van Gelder, 1991). Often, these associations are characterised by similar interests, common goals and philosophies.

Applying this research on a meta-theoretical level, investigators have begun to construct paradigms for the Internet which place it beyond the confines of technology. The language that is overwhelmingly employed is that of community. Quarterman (1993) uses this term when describing the vast array of political, social and economic activities occurring on the network. Kumon and Aizu (1993) note that networked communications “present a new social system that people join in order to share useful information, knowledge, and even wisdom and in which the dominant form of social interaction is persuasion/inducement”.

The trend establishing the Internet as a type of community also links it to a major theme of ethical analysis. Medical ethicist Tristam Englehardt (1986) credits the eighteenth century philosopher, Immanuel Kant, with shifting the study of values from a search for insight into the mind of a deity to the consideration of common, regular experiences of society. This enduring approach emphasises the abilities of a community to perceive in its experiences a sense of the ethical and that these perceptions may be rationally described. Alisdair McIntyre (1981) echoes these notions in stating that “a moral philosophy ... characteristically presupposes a sociology” since “every moral philosophy offers explicitly or implicitly at least a partial conceptual analysis of the relationship of an agent to his or her reasons, motives, intentions and actions, and in so doing generally presupposes some claim that these concepts are embodied or at least can be in the real social world.”

A more empirically-based rationale for community as a basic unit of ethical discernment is captured by Philip Selznick (1992). He observes that it exists as a framework in which people sharing the same beliefs, interests and goals “establish a common faith or fate, a personal identity, a sense of belonging, and a supportive structure of activities and relationships”. Based on the fit of the foregoing CMC research with standard sociological definitions, it is not unreasonable to associate the emerging activities of the Internet with the dynamics of a community.

Evaluating the Internet in this manner achieves several desirable goals. First, there is the benefit of accuracy as measured by behavioural and social research. This provides a degree of fairness in the portrayal of what ethical questions are extant within the CMC environment. Second, it allows for an expanded contextual analysis of that issue. It avoids the problem of techno-centric relativism by assessing situations against a larger background of community dynamics. Finally, it provides a relatively stable means of analysis by locating the effects of the behaviours within the immediate environment of their impact. This can avoid the need to apply any number of ‘real world’ analogies to CMC which may either be attenuated (e.g. the Internet is like broadcast television) or plainly incorrect (e.g. the Internet is like a park-side soapbox).

With these baselines established, it remains to apply the concept of community to specific issues currently evolving on the Internet. While a complete recitation is beyond the scope of this paper, and indeed rendered nearly impossible by the dynamic nature of the Internet, there are several areas which merit consideration within the context of community-based analysis.

3 VIRTUAL VERSUS TANGIBLE OBJECTS

In his classic study of the liberal-democratic state, MacPherson (1962) claims that at its roots, “political society becomes a calculated device for the protection of this property and for the maintenance of an orderly relation of exchange”. It takes minimal analytic effort to recognise that tangible objects consume much ethical and legal attention. Margaret Radin (1993) notes that the reasons for this focus go beyond the need to possess and transfer physical goods for economic purposes and reaches to our understanding of personhood itself.

While society has conferred value upon such intangible objects as speech, artistic works and ideas, the Internet has thrust these “virtual” constructs into a new and compelling light. Anne Wells Branscomb (1994) recognises this situation when she writes that “the infrastructure established to govern the fruits of the industrial age — intellectual property laws (patents, copyrights, and trade secrets) — are stretched, some of them to their limits, by new forms of creative endeavour such as computer software interfaces, which do not appear to fit comfortably into any one of the existing legal categories”.

THE AUSTRALIAN COMPUTER JOURNAL, VOL. 29, No 1, FEBRUARY 1997
Immediately apparent is the fact that CMC’s very existence is defined by the non-physical. Michael Heim (1994) does not exaggerate matters by stating that “computer culture interprets all knowable reality as transmissible information”. This stands in stark contrast to conventional thought which tends to evaluate information as an object within a larger social sphere. Copyright law, for example, treats information as a commodity for exchange. Expression such as speech or writing is often protected for its role in enhancing the democratic process.

As the Internet continues to evolve, various interests will compete in attempting to define the meaning of information. One popular theory claims that CMC accentuates the need to view information as an important economic asset and to accord increased proprietary protections. This view has recently inspired the United States Congress to introduce the National Information Infrastructure (NII) Copyright Protection Act of 1995.

The NII Act as currently written, would create a right of “digital transmission” which would protect copyrighted information within networks such as the Internet. Specifically, it would allow the imposition of civil and criminal penalties upon individuals who download protected information without permission.

This legislation has been criticised for broadly prohibiting any use of copyrighted information. For example, the current Act seemingly contains no provisions for the downloading of such material for non-profit, personal use. This exception, which exists in traditional copyright schemes and is known as the “fair use doctrine” has thus far been left out of the digital counterpart. Critics of the bill warn that this omission will eviscerate the information-intensive environment of the Internet by placing unprecedented restrictions upon interchange (Love, 1996).

A detailed analysis of this legislation is beyond the scope of this paper. However, several features demonstrate the problems which accompany a purely technological approach to issues which have wider, human implications. This is most apparent in the reasons surrounding the absence of “fair use”.

According to an analysis of reasons behind the exclusion “fair use”, one overriding consideration was the heavily technical interpretation of the act of “fixation”. Within copyright law, a creation is “fixed” when it has taken some form in which people can perceive it (Strong, 1995). Once “fixed”, it enjoys copyright protection. Traditionally, this concept has been linked with tangible mediums which preserve the work so that it can be perceived by others. Current copyright changes contemplate the granting of fixation status to any situation in which any information is “transmitted” by a computer for any length of time. Accordingly, any user could be liable for downloading any stored information regardless of how long it has been online or for what purpose it has been downloaded (Okerson, 1996).

If passed into law in its current format, copyright law could nearly eliminate or severely restrict the casual access of any online document. This will be accomplished by the fact that the act of transmission of digital information has been elevated above its purpose. A community-centred approach would seek to place actions occurring within the virtual environment in a broader context. Activities which require the transmission of data, such as browsing a Web site would be deemed the equivalent of the perfectly legal perusing of a book or periodical in a bookstore and would not be prohibited.

Similarly, using the same technological blunders as applied to fixation, the currently contemplated version of the legislation would eliminate what is known as the doctrine of “first sale”. This concept in its conventional application allows for the reselling or giving of books or periodicals to others without having to pay additional royalties to the copyright owner. An obvious social benefit of this arrangement is the wide dissemination of intellectual works. Under the “transmission” theory of data, this benefit no longer exists in the electronic environment since a work will be fixed at each transmission. Again, such an outcome is avoidable if legislators accentuate the community-centred aspects of the issue and consider the negative impact which such a restriction would have upon the overall intellectual climate.

The current changes contemplated within United States copyright law demonstrate the outcome of a standard which cleaves technology from the fundamental behaviours of a community. They represent a failure to incorporate policies in an electronic context which have been obvious to lawmakers in more settled environments. In so doing, a wealth of available insights and norms acquired from our historical experiences are needlessly lost and the resulting legislation which lacks commonsense appeal, loses any precedential value and claim to integrity.

In competition with a “proprietary” theory of information is the notion that all data, regardless of its character, should be freely disseminated along the Internet. Not surprisingly, criticism of this stance is equally prolific as that levelled at its counterpart. While a community-based analysis will not provide a simple resolution to this conflict, it can help to provide insight as to both the context of the problem and the effects of proposed resolutions upon the overall structure of the CMC environment.

4 VIRTUAL VERSUS TANGIBLE PERSONAS
Along with changes in the possessory nature of information, the Internet is causing shifts in the way that we view ourselves. This was brought home several years ago in the now famous episode in which a New York psychiatrist successfully held himself out to be an elderly woman on the Internet. When exposed, this situation caused a range of emotions, from shock to rage (Van Gelder, 1991).

The impersonation case is a poignant, but not uncommon reminder that many of the usual cues associated with identity are not present within virtual spaces. One aspect of this “virtual anonymity” has been the removal of such barriers to communication as gender, race, physical handicap and cul-
tural orientation. These developments have been identified as factors which can enhance the exchange of information and engender cooperation and understanding on a global scale (Walls, 1993).

There is, however another side to the “virtuality” of identity which deals with the information surrounding individuals. With online personas constituted as so many data points, it becomes possible to dissect it by bits and pieces with relative ease.

An example of this issue was recently raised in the United States by the Center for Media Education (1996). In a report concerning the development of market “tracking technologies”, the Center detailed various methods by which the interactive tools of the Internet have been used to gather information about the consumer habits of children. According to the report, the ultimate goal of this effort is the “microtargeting” of this population by eliciting data through electronic environments “designed to capture a child’s attention”.

The potential for computer-based, interactive platforms to collect information on young and old alike without knowledge or consent is obvious. Branscomb (1994) lists what only can be imagined as the most obvious areas of concern such as telephone numbers, addresses, entertainment preferences and religious convictions. Collection can occur through any number of means, including the surreptitious. Currently, it has not been determined in law or policy as to what can be collected and by what means.

The quandaries posed by information gathering are not confined to the means employed or the straight dissemination alone. In legal theory, it has been suggested that in the near future, a cause of action may need to be developed to combat negligent or intentional mischaracterisation of data composited from electronic mediums (Smolla, 1993).

Much of the debate concerning what data can be collected and how it will be used will hang on an understanding of what constitutes the zones of an individual’s virtual identity. While agreement may seem far off, the implementation of a community-based analysis may be helpful in giving isolated data points a context within the larger environment. Branscomb (1994) advises that many of the problems underlying debates about information in this new environment are the result of our lack of experience in agreeing upon acceptable behaviour. The addition of the wider perspective afforded by consideration of community dynamics can work to improve upon the available fund of knowledge.

5 VIRTUAL VERSUS TANGIBLE BORDERS

The concept of privacy is a thread which runs through these issues. Like communications technology, privacy as an articulated value is of a relatively recent vintage. It was not until 1890 that Samuel Warren and Louis Brandeis wrote about “the individual’s right to be left alone”. Before this time, the matter was treated in conjunction with other issues such as property and interference with personal zones. The historian Leónard Levy (1988) observes that, in colonial America, the term was unused as such, but was couched in concepts of physical security against government intrusion.

The relative newness of privacy should arguably make it amenable to modern circumstances, but this has not always proved to be the case. In American law, assertions of privacy against communications innovations have been held unfounded. For example, in Olmstead v United States (1927), the Supreme Court first considered the privacy expectations accorded to telephone users and held that none existed. Specifically, the Court reasoned that the installation of the telephone wires which reached from one’s home or office “to the entire world” could not be practically granted under the Constitution.

While a right of privacy against governmental wiretaps was finally recognised in 1967, the Court has continued to apply a cautious approach to claims involving technological devices. In Smith v Maryland (1979), the Court held that no invasion occurred when a device was attached to a phone line in order to collect outgoing numbers. Such information was, in the Court’s opinion, necessarily disclosed to the telecommunications operator to reach the other party and thus could not be expected to be private. Significantly, subjective expectations about the private character of these transmissions were dismissed with little comment.

Until recently, the privacy of cordless telephones was a subject of split opinions within the United States. A majority of state and federal courts reasoned that no such right could be inferred as the voice content was transmitted through easily-monitored AM radio waves. According to these decisions, the simplicity of interception should be known by all cordless users and thus could not be expected to be private (Tyler v Beroldt, 1989). A minority of states which declined to follow this exclusion did so largely by noting “the vital role that the cordless telephone has come to play in private communications” (Connecticut v McVeigh, 1993). The matter has now been settled by a federal statute according protection, but the contrasts in rationale remain instructive.

Although culled from American jurisprudence, these opinions reflect a wider interpretation of these issues which places privacy within a confines of technological function. Wires which reach the world cannot be reasonably regarded as private. Digits which are necessary to gain access to telephone numbers must be considered surrendered to the world. In both instances, the paradigm emphasises the physical characteristics of the medium and assumes that these parameters will be known and respected by their users.

This techno-centric approach may soon find its way into such virtual privacy issues as those presented by electronic mail or similar methods. In general, the claim begins with the statement that the architecture is readily-susceptible to intrusion. From this premise, it is posited that the use of electronic mail is accompanied by the inherent risk of unanticipated disclosure. If accepted, the position would invalidate any reasonable expectation of privacy.
Theories which place primary emphasis upon hardware configurations are appealing because of their simplicity. They are also dangerous as they artificially limit value choices. Although presented in terms of the technologically feasible, they are ethical in nature and involve more factors than the configurations of the hardware at issue. The use of a community-based analysis avoids the trap of techno-centric limitation and places the inquiry within the broader scope of human ethical experience and values.

6 CONCLUSION
The Internet is in many ways a new phenomenon. As such, it presents society with a seldom-experienced opportunity to formulate laws and policy which will be responsive to its needs. However, although many issues are cloaked in the ultra-modern language of technology, the majority of these challenges raise basic ethical questions which may best be addressed by looking to a primary source of ethics as well as law: the values and dynamics of community. In so doing, we maintain contact with a rich resource of ethical thought which has spoken to many of these questions and may again be called upon to provide comprehensive and coherent responses. As with any significant phenomenon, the genesis of a jurisprudence which reflects integrity and encourages international recognition will be best developed through the participation of the wide variety of users who populate this new frontier.

REFERENCES
Smith v Maryland, 442 U.S. 735 (1979).
Tyler v. Bertoti, 877 F.2d 705 (8th Cir. 1989).

BIOGRAPHICAL NOTES
Brian M O’Connell is an attorney and is on the faculty of Central Connecticut State University, New Britain, Connecticut. He received his undergraduate degree in Philosophy and Psychology from Trinity College, Hartford and a Juris Doctor degree from the University of Connecticut School of Law. He is a member of the United States Supreme Court Bar and of the Connecticut State and Federal Bars. His current research interests include the jurisprudence of new technologies.
INTRODUCTION

The coming into being of the Internet has generated a number of ethical problems, and some of the more pressing concern the moral notion of privacy. Some of these problems arise from greater access to new data bases. For example, a hacker in Europe can access a university data base in the USA. Another cluster of problems revolves around the threat to privacy posed by new possibilities of monitoring and surveillance. For example, law enforcement officials can intercept the electronic messages of suspects who in fact may not be guilty of any crime.

The provision of an adequate philosophical account of the notion of privacy is a necessary precursor to setting the proper limits of intrusion on the Internet. Such an account of privacy would assist in defining the limits to be placed on unacceptably intrusive activity. Moreover it would do so in such a way as to be sensitive to the forms of public space created by the Internet, and not unreasonably impede those new possibilities of communication and information acquisition which are in fact desirable. As always it is important to balance the rights of individuals against the needs of the community. On the one hand there is a fundamental moral obligation to respect the individual’s right to privacy, on the other hand there are the legitimate requirements of, for example, law enforcement agencies to monitor the communications and financial transactions of organised crime. Moreover the working out of these ethical problems is relative to a particular institutional and technological context. The question as to whether e-mail, for example, ought to be assimilated to ordinary mail depends in part on the nature of the technology in question and the institutional framework in which it is deployed. Perhaps e-mail messages sent on a company-owned computer network ought to be regarded as public communications within the organisation however personal their content since, unlike ordinary mail, e-mail messages are always stored somewhere in the backup system owned by the company and therefore are accessible to the dedicated company cybersleuth (Magney, 1996). I will begin with an outline of the general notion of privacy (Warren and Brandeis, 1980; Benn, 1988).

The notion of privacy has proven to be a difficult one to adequately explicate. However, there are a number of general points that can be made. First, the notion of privacy has both a descriptive and a normative dimension. On the one hand privacy consists of being in some condition of not being interfered with or having some power to exclude, and on the other privacy is held to be a moral right, or at least an important good. Most accounts of privacy acknowledge this much. For example, Warren and Brandeis gave an early and famous definition in terms of the right to be let alone. Naturally the normative and the descriptive dimensions interconnect. What ought to be must be something that realistically could be. The normative dimension of privacy is not a fanciful thing. We need to reject the proposition that the extent and nature of the enjoyment of rights to individual privacy is something to be determined by the most powerful forces of the day, be they...
market or bureaucratic forces. But it is equally important to avoid utopian sentimentality; it is mere self-indulgence to pine after what cannot possibly be.

Second, privacy is a desirable condition or power or a moral right that a person has in relation to other persons, and with respect to the possession of information by other persons about him/herself or the observation/perceiving of him/herself by other persons. The kind of ‘interference’ in question is cognitive or perceptual (including perhaps tactile) interference.

Third, the range of matters regarded as private embraces much of what could be referred to as a person’s inner self: a demand — as opposed to a request — by one person to know all about another person’s thoughts, beliefs, emotions, and bodily sensations and states would be regarded as unacceptable. Naturally there are conditions under which knowledge concerning another person’s inner self are appropriate. A doctor needs to know about a patient’s bodily sensations and states, in so far as this was necessary for successful treatment and in so far as the patient had consented to be treated. Here part of the sphere of an individual’s privacy (the patient) has been widened to include another person (the doctor) in virtue of the need to establish a professional medical relationship. Nevertheless such information, while no longer unavailable to the doctor, would still be unavailable to others, and for the doctor to disclose this information would constitute a breach of confidentiality. More generally, people are entitled to know of a person’s intentions and beliefs in so far as these are likely to lead to actions which will affect their interests.

Fourth, a person’s intimate personal relations with other people are regarded as private. So while a lover might be entitled to know his/her lover’s feelings toward him/her others would not be so entitled. Indeed there would typically be an expectation that such information would not be disclosed by a lover to all and sundry.

Fifth, certain facts pertaining to objects I own, or monies I earn, are held to be private simply in virtue of my ownership of them. Ownership appears to confer the right not to disclose information concerning the thing owned. Or at least there is a presumption in favour of non-disclosure; a presumption that can be overridden by, for example, the public interest in tax gathering.

Sixth, certain facts pertaining to a person’s various public roles and practices, including one’s voting decisions are regarded as private (Benn, 1988). These kinds of facts are apparently regarded as private in part in virtue of the potential, should they be disclosed, of undermining the capacity of the person to function in these public roles or to fairly compete in these practices. If others know how I vote my right to freely support a particular candidate might be undermined. If business competitors have access to my business plans they will gain an unfair advantage over me. If a would-be employer knows my sexual preferences he or she may unfairly discriminate against me.

Seventh, and more generally, a measure of privacy is necessary simply in order for a person to pursue his or her projects, whatever those projects might be. For one thing reflection is necessary for planning, and reflection requires privacy. For another, knowledge of someone else’s plans can enable those plans to be thwarted. Autonomy requires a measure of privacy.

Eighth, the data owned, and ‘actions’ performed, by organisations and groups — including businesses and government agencies — or by individual persons in their capacity as members of organisations or groups, may also be regarded as private, or at least confidential, and for some of the reasons given above. For example, a business company needs a measure of confidentiality in relation to its plans if it is to be able to compete on equal terms in the marketplace. Again law enforcement agencies must retain confidential information in relation to the activities of criminal organisations.

Equipped with this working account of privacy, including a basic taxonomy of the kinds of information regarded as private or confidential, let me now consider three different kinds of ethical issue that arise in relation to the Internet.

The first set of issues arise when an unauthorised person accesses private or confidential data, such as an organisation’s or an individual’s financial, medical or criminal data or records, via the Internet.

The accessing of a person’s personal data or an organisation’s confidential information by someone who is not entitled to that access is an invasion of privacy and as such prima facie morally wrong. Naturally, there are exceptional circumstances in which although an invasion of privacy is prima facie morally wrong it is for a higher good, and this consideration overrides the right to privacy. However, it needs to be stressed that such cases are exceptional, and a convincing justification would need to be available in each case. Such justification would necessarily rely on some moral consideration which had greater moral weight than the right to privacy in the circumstances.

The accessing of personal or confidential data is not only a (prima facie) moral wrong in itself. For such accessing can have harmful consequences if the data accessed gets into the wrong hands or if the data is false or both. For example, a person with a criminal record might be denied a job opportunity by an employer unlawfully in possession of information concerning a crime committed by a job applicant decades previously. Again, a seller unlawfully in possession of false credit information might refuse to sell to a buyer.

It is sometimes suggested that infringements of privacy are not morally wrong if the person whose privacy is invaded does not know about it and if there are no harmful consequences. However, I have argued that persons have a right to privacy and that therefore an unauthorised invasion of that privacy is a prima facie moral wrong, irrespective of whether the person knows his/her privacy has been invaded, and irrespective of the harmful consequences. The point is simply that the invader is in possession of information, or has made observations, which he or she does not have a right to possess or to make; indeed he or she has acquired that information or made those
observations in violation of the privacy rights of someone else. If I steal someone’s property I have still committed a wrong notwithstanding the fact that they may never notice that the item has gone missing.

Unauthorised access to private or confidential data also raises other questions. Should the data have been collected in the first place? One concern here is the increasing tendency for some government agencies to undertake the integration of data bases initially gathered and held by other government departments for specific purposes, and use the resulting information for new purposes (Kusserow, 1995; Shattuck, 1995 and Clifford, 1995). Another is the coming into existence of data bases built up as a result of profiling. This involves using an existing bank of data to develop a set of criteria definitive of the ‘profile’ of say, a typical offender, and then using this profile to select from a large number of individuals those who fit the profile, and therefore qualify for further investigation.

The unprecedented growth in data bases on individuals by government agencies and corporations raises the spectre of an increasing information imbalance between private citizens and governments and between private citizens and corporations (Rule, 1995). This imbalance is to some extent redressed through individuals’ access to the Internet, and to encryption products, and also by privacy legislation enabling such things as access to government data bases, files on individuals, and so on. Moreover, there are new technologies, such as smart cards, whose future impact on this imbalance remains unclear. Nevertheless, overall there appears to be an increasing informational imbalance and it entails a shift in the balance of power between ordinary citizens and organisations. Obviously any increase in the power of organisations, including corporations and governments, has profound implications for individual rights, including especially autonomy. For rights cannot be adequately exercised by those with diminishing power.

Other questions concern the status of the person who has accessed the data and the accountability of those who have authorised access. What kinds of person ought to be authorised in relation to a specific category of data, and what forms of accountability ought to be in place? As we saw above, personal financial information is regarded as private by virtue of its ownership by the person to whom it pertains. Nevertheless it is obviously legitimate for, say, lenders, to be aware of the credit record of their would-be customers. However, lenders are only entitled to certain private financial information if they need it for a legitimate purpose - say, to ensure credit-worthiness - the customer is prepared to freely disclose it, the customer has access to it, and so on. Thus, car sellers are not morally entitled to detailed knowledge of the assets and liabilities of members of the public simply because it would be useful in terms of their marketing or sales initiatives. Moreover, authorised personnel need to be held accountable for ‘onselling’ confidential data, and other related activities. One of the problems in this whole area is the extent to which accountability is in fact a realistic goal given the extent of data that has been gathered, the numbers of authorised personnel who have access to it, and the interconnection between data bases made possible in part by the Internet.

The second set of issues concerns the accessing of data and/or intercepting of communications on the Internet by law enforcement officials.

The notion that privacy is an absolute right that cannot be overridden under any circumstances is unsustainable, whether it be privacy on the Internet or on any other communication or information system. The rights to privacy of some individuals, and the right to confidentiality of members of some organisations, will in some cases be overridden by the rights of other individuals and other members of organisations to be protected by the law enforcement agencies from the perpetrators of serious crimes, such as murder, child pornography, drug trafficking, armed robbery and fraud.

Moreover, the rights to privacy of some individuals and/or confidentiality rights of members of organisations can in some instances be overridden by the community’s interest in computer security. Consider in this connection programmers who devise and release destructive viruses and worms which infiltrate strategic government and economic computer systems via the Internet. Consider also the communications of drug dealers, pederasts, saboteurs and terrorists. These communicators have an interest in sophisticated forms of encryption. Correspondingly, law enforcement agencies have sought to have access to ‘plain text’ versions of encrypted communications for the purposes of tracking down such persons (Levy, 1995).

In relation to accessing of data and/or intercepting of communications on the Internet by law enforcement agencies a balance has to be struck between rights to privacy and confidentiality on the one hand and the rights to protection from serious crime on the other. Moreover, the state of technology at any point in time to some extent determines the possibility of striking a balance. For example, the current availability to the general public of very secure computer systems and of high level encryption products makes accessing of data and/or intercepting of communications on the Internet by law enforcement agencies extremely difficult and expensive. At any rate in striking this balance a number of principles need to be kept in mind.

First, because such accessing and/or intercepting are by definition an infringement of privacy the presumption must be against their use. That presumption can be overridden in particular cases or by exceptional circumstances such as in wartime, but not by a blanket appeal to the common good or to the need for security.

Second, the benefits of such general practices must offset the costs, including the costs in terms of the erosion in public trust. As the East European experience under communism has taught us, high levels of monitoring, surveillance and detailed record keeping are inconsistent with an open free society based on trust between public bodies and private citizens.

THE AUSTRALIAN COMPUTER JOURNAL, VOL. 29, No 1, FEBRUARY 1997
Third, the accessing and/or interception in question is in relation to a serious crime; there is reasonable suspicion that the person whose privacy is to be invaded has committed the crime and that the resulting information is likely to substantially further the investigation in relation to that crime.

Fourth, there is no alternative method of gathering the information which does not involve an invasion of privacy.

Fifth, the law enforcement officials are subject to stringent accountability requirements, including the issuing of warrants in circumstances in which the justification provided is independently adjudicated.

Sixth, those whose privacy has been invaded will be informed that it has been invaded at the earliest time consistent with not compromising the investigation, or related investigations.

In addition to these general principles, there are particular considerations in play in relation to encryption. On the one hand the proposal that law enforcement agencies have automatic access to the "plain text" decoder of all encryption products violates the presumption in favour of privacy.

On the other hand, interception and/or accessing might be legitimate if individuals have recourse to a kind and extent of security in respect of their communications and data which is: (a) clearly in excess of the legitimate security requirements of ordinary citizens, and out of all proportion to the threats posed to the privacy of ordinary citizens, and; (b) known to be used by criminals, terrorists and so on for the conduct of illegal activities. Such a kind and extent of security constitutes grounds for reasonable suspicion, or at least does so in the absence of special justification. An example here might be the use of higher level encryption products without adequate justification.

The third set of issues concerns the monitoring and surveillance of employees who might be accessing the Internet for illegitimate purposes, such as viewing pornography during worktime. Once again employees do not have an absolute right to privacy in their place of employment. They are to some extent accountable for their actions to their employers, and accountability entails some measure of monitoring in the workplace.

It goes without saying that the information acquired by employers concerning their employees ought not to consist of personal data unconnected to their employee's work. However there also needs to be limits placed on the accessing and/or interception of computer communications which are work related. Academics sending e-mail messages to overseas colleagues in relation to their research are not legitimate targets for university administrators concerned with workplace reform. Work related information is protected by privacy and related rights in the following ways.

Firstly, employees have specific roles within organisations which entail confidential relationships. For example, a lawyer has a confidential relationship with his client, and the lawyer's employer has no right to breach that confidentiality simply by virtue of the fact that he or she is the employer.

Secondly, as we saw above, privacy is both a right in itself, and a necessary condition for autonomy — a measure of autonomy in their work, as elsewhere, being a fundamental right of employees. Employees do not lose their basic moral rights, including rights to privacy and autonomy, simply because they are employed. Indeed, ultimately such rights have greater moral weight than the right of employers to monitor their workforce. At any rate, here as elsewhere, a balance has to be struck between the rights of employers to hold their employees accountable and the rights to privacy and autonomy of employees. In short, excessive monitoring and surveillance is unacceptable, being a violation of the right to privacy and autonomy.

Finally, there are pragmatic arguments for limiting workplace monitoring and surveillance. Such monitoring and surveillance may have costs in terms of resources used and the level of anxiety generated in the employer's workforce. Moreover, it may undermine the trust relationship between employer and employee. The cumulative impact of these costs may far outweigh the gains in accountability, and there may well be a net financial loss to the employer.

REFERENCES

BIOGRAPHICAL NOTE
Seumas Miller is Professor of Social Philosophy, and Head, School of Humanities and Social Sciences, Charles Sturt University, Wagga Wagga. He has research interests in professional and applied ethics. He has recently co-authored two books entitled, respectively, Rethinking Theory (Cambridge University Press), and Police Ethics (Allen and Unwin).
Australian Approaches to Internet Content Regulation

James M Hogan
School of Computing Science,
QUT, GPO Box 2434, Brisbane 4001
hogan@fit.qut.edu.au

Peter CJ James
Allen, Allen and Hemsley,
Riverside Centre, 123 Eagle Street,
Brisbane 4000
peter.james@aahq.access400.aone.net.au

Concern over access by minors to undesirable material over the Internet has led to a flurry of regulatory activity by Australian governments since 1993. This article examines these responses in the context of the existing law — focusing upon the development of appropriate legislative models for on-line services and content classification. Many of these approaches require some level of self-regulation through Industry Codes of Practice, and we examine the likely requirements of such codes, their role in limiting liability of service providers for the transmission of prohibited material, and the potential for legal and ethical breaches by computer professionals as a result of compliance with code provisions.

1 INTRODUCTION

The issue of Internet content regulation has been actively considered by Australian governments since late 1993, through a succession of inquiries (including those of a Senate Select Committee) and legislative efforts culminating in the July 1996 report of the Australian Broadcasting Authority On-Line Services Inquiry (ABA, 1996b). Following the lead of the Broadcasting Services Act 1992, these documents propose that the on-line industry should in most respects be self-regulating through government registered Codes of Practice (COPs), with appropriate criminal sanctions for breaches of “community standards” (ABA, 1996b) in regard to restricted or objectionable material. In October 1996, the Federal Government announced legislation significantly expanding the role of the ABA to include on-line services, with authority over COPs for the industry (Fin. Rev., 1996b). The ABA has indicated that only COPs consistent with its published guidelines (ABA, 1996b) will be eligible for registration, and while exact requirements remain uncertain, compliance has the potential to generate numerous ethical concerns for computer professionals — especially for systems administrators — and to add significantly to their responsibilities.

This paper is, therefore, intended to provide a summary and analysis of the present state of Internet content regulation in this country, along with the necessary legal context provided by legislation governing existing media. As far as possible, these issues are examined independently from the general censorship debate, and so two assumptions underlie our approach:

(i) There exist necessary limits upon freedom of speech; these should be as tightly constrained as possible and extensions rigorously justified.

(ii) Censorship provisions should be as consistent across modes of delivery as possible, and unless new technology fundamentally alters the nature of contentious material, the governing consideration should be the level of control over inadvertent access — especially access by minors.

The remainder of this section provides some background to the issues and to the regulatory challenges posed by the nature of the Internet. Section 2 briefly introduces the technology and the associated terminology, providing both an introduction to the existing censorship provisions and an examination of their suitability in the on-line context. This is followed in Section 3 by an analysis of the overall regulatory framework, and of problems associated with draft COPs as exemplified by that of the Internet Industry Association of Australia (INTIAA, 1996) — our conclusions being summarised in Section 4.

Copyright© 1997, Australian Computer Society Inc. General permission to republish, but not for profit, all or part of this material is granted, provided that the ACJ’s copyright notice is given and that reference is made to the publication, to its date of issue, and to the fact that reprinting privileges were granted by permission of the Australian Computer Society Inc.

Manuscript received: April 1996

1 Broadly speaking, “restricted” material is that which a reasonable adult would regard as unsuitable for a minor, whereas “objectionable” material is more likely to cause great offence — for example RC (Refused Classification) films, games or publications, child pornography or material promoting or inciting crime or violence. Details are available at the Office of Film and Literature Classification Web page (OFLC, 1996).
1.1 Background Information

Much of this article is concerned with the adaptation of regulatory approaches for existing media to the new technology of on-line services. While censorship was introduced in the context of printed publications, content regulation has developed to encompass new technology as it has become available. Usually, new technology does not of itself fundamentally change the nature of contentious material, and so the challenge for the modern legislature is to respond to the greater population coverage and ease of access afforded by advances in broadcasting and telecommunications.

Yet the Internet and similar technologies provide greater challenges than before, as for the first time Australian governments are faced with a means of importation of contentious material that cannot realistically be controlled at the borders through inspection by customs officers or other law enforcement officials. While this flexibility is also the technology's virtue, it is inevitable that regulation of this environment will place substantial demands upon computer professionals — both in the context of detection and reporting of possible infringements of the law, and in the gathering of evidence for possible litigation or prosecution.

The quantity of material available through the Internet is vast, and only a small fraction (Senate Committee, 1995b; ABA, 1996b) of it would be likely to be classified restricted (R,X) or refused classification (RC) under the existing OFLC scheme — the OFLC view being that the bulk of this material is accessible through clearly labelled Usenet newsgroups and disjoint bulletin board services rather than through the World Wide Web.

However, initial action by Australian governments was driven by concerns by various organisations and (at times hysterical) media reports about access by unsupervised minors to contentious material, and early approaches reflected this fact, with the Senate Committee (1995b) recommending legal prohibition of on-line material at the restricted (rather than RC) level, and an ill-considered New South Wales Bill placing the threshold even lower. The NSW provisions, which were under consideration as "model" legislation for all states and territories, have subsequently been abandoned (Fin. Rev., 1996a) in favour of co-operative development of uniform state legislation in conjunction with the ABA. This approach is highly desirable if unfortunate cross-jurisdictional prosecutions such as the American Thomas case (prosecution of an offender in one state for accessing material lawfully placed on-line in another) are to be avoided in Australia (Senate Committee, 1995b).

The focus of legislative control under the ABA regime has shifted towards RC material such as child pornography, a change reflected in the recommendation that RC be maintained as the legal threshold for on-line documents (ABA, 1996b). However, the ABA remains of the view that such legislative prohibitions are necessary, concluding, despite extensive submissions from Internet users, that traditional "netiquette"-based approaches are inadequate to address either set of concerns.

Of course such legislation may at present be applied only to those within Australian states and territories, and many of those responsible for creating contentious material lie outside its reach. Of further concern to regulators must be the constant evolution of Internet technology and usage — for example, the current proliferation of on-line digital video and related services — and the technical difficulties inherent in authenticating usage to a point at which a conviction may be obtained. Enforcement will thus be difficult (and in some cases virtually impossible) without international agreements and regular review of the regulatory framework.

2 APPROPRIATE LEGISLATIVE MODELS FOR THE INTERNET

2.1 On-Line Services

Censorship provisions are necessarily concerned with the content delivered through a particular medium, and, in the case of the Internet and related technologies, it is necessary to make strong distinctions between the responsibilities of originators of material and suppliers of network infrastructure and computing services — distinctions which currently apply in telecommunications — although it must be noted that a number of vendors (such as Telstra and CompuServe) operate businesses which straddle these distinctions.

In this paper, we adopt definitions similar to those of the ABA (ABA, 1996b):

(i) Content providers: any party who publishes material in the on-line environment — whether the party is the author or originator of the material or merely acts as a distributor of it (such as a University providing an Internet accessible repository of technical reports).

(ii) On-Line Access or Service Providers (ISPs): organisations or vendors offering access to an on-line computer service — usually via modem to a powerful server which may provide a gateway to other networks (such as the Internet). In particular, this definition does not include the provision of the underlying network infrastructure (iii), below). Examples include On Australia, America On Line and Ozemail.

(iii) Network infrastructure providers: licenced vendors responsible for the provision of telecommunications carrier services, such as Telstra and Optus.

A further distinction is commonly made between 'open' and 'closed' systems — in the sense of access limitations and isolation from other networks, and in regard to whether all users or only a nominated person or organisation may provide
content to the system. If, as recommended (Senate Committee 1995b; ABA, 1996b), future legislation of COPs require service providers to restrict access only to adults, these distinctions become superfluous — excepting perhaps the possibility of local ‘adult’ services licenced in the same way as restricted bookshops and requiring submission of content to the OFLC for classification although there is little support for this among censorship ministers (Edwardes, 1996).

More troublesome is the task of drafting regulations so as to cover the numerous activities that together constitute on-line services. Much of the discussion below is concerned with material usually carried through bulletin board and World Wide Web facilities, but consideration must also be given to real time chat services (such as IRC) and email. The ABA is strongly of the view (ABA, 1996b) that private email should be exempt from any content classification and, to the extent that regulation may be necessary, an appropriate mechanism is that provided by the Crimes Act 1914, Section 85ZE:

A person shall not knowingly or recklessly:
(a) use a telecommunications service provided by a carrier to menace or harass another person; or
(b) use a telecommunications service provided by a carrier in such a way as would be regarded by reasonable persons as being, in all the circumstances, offensive.

... provisions which carry a penalty of imprisonment for one year. The situation is more complicated in the case of chat lines, and email sent to multiple recipients. In this situation, some limited application of the publication model discussed below may be reasonable, although pre-classification is unworkable. The ABA Report (1996b) suggests that the “test of the degree to which an on-line service should be regulated should be the extent to which it may be said to be intended for public access" and, at the margins, such issues must be determined on a case-by-case basis.

2.2 Current Australian Legislation

Censorship has received legislative attention in different forms throughout Australia, typically addressing printed publications initially, with new provisions being enacted to address the censorship challenges of film and video tape as technology evolved. The federal government’s Classification (Publications, Films and Computer Games) Act 1995 (the “Federal Act", given assent on 15 March 1995) regulates classification in the ACT and was intended to be the legislative model for use by each State and the Northern Territory, under which responsibility for performing classifications would be undertaken at the federal level using a uniform National Classification Code. Although not entirely uniform, complementary State legislation has been enacted in most states and the Northern Territory.4

Despite these statutes being directed towards publications, films and computer games, the definitions used are generally wide enough to encompass on-line materials, provided they do not constitute broadcasting services under the federal Broadcasting Services Act 1992 — although for example the Queensland Act explicitly excludes a “bulletin board” from the definition of a “computer game”. Nevertheless, the Western Australian, Northern Territory and Victorian laws attempt to specifically extend the legislative reach to computer services or on-line transmission of objectionable material, and the now-abandoned New South Wales model had similar provisions.

2.2.1 Existing Classification Criteria and the Internet

If the existing OFLC classification system is to be applied to works uploaded, transmitted or downloaded via the Internet, it is necessary to determine whether material accessed on-line should be characterised as a publication, film or computer game or as some combination of these. Whilst the criteria for classification of each of these expressions each involve a degree of complexity in determining the resulting classification level, the task is even more difficult in an on-line context where a single transmission might include written or pictorial matter (normally a “publication”), video information and visual images (normally “film”) and computer games. Of course, usually the medium (film, tape or paper) assists characterisation, but this is obviously not applicable in the face of purely digital forms. Apart from the development of a new classification model to encompass all on-line content (Section 2.2.2.), the alternatives are:

(i) To choose one of the classification groupings to apply to all on-line transmissions. Under this alternative, all transmissions might be required to be classified (for example) as publications, irrespective of whether the document had been digitised from film or some other medium. This eliminates multiple classification problems but also presents difficulties and anomalies — the most serious in the selection of the model. An overarching publication model is more easily adapted to on-line documents than the other categories and it has already been judicially accepted as an appropriate concept to describe on-line data distribution and BBS functions5 — albeit for purposes other than classification. However, this approach would inevitably result in some loss of flexibility as categories for existing media would be lost, and some confusion may result if the on-line version of a film or computer game were to carry a different classification from those in the traditional media.

(ii) To apply each of the classification criteria to different parts of a single on-line work. The application of the different categories of classification to different aspects

---

4 Details of the relevant Acts and their respective dates of assent may be found in Hogan and James (1996).

5 For example, defamation cases in Western Australia (Rindos v Hardwick, Ipp J., Supreme Court 31 March 1994) and in the USA (Stratton Oakmont v Prodigy Services Company 23 Media L Rep 1794).
of an on-line work has the advantage of consistency, but may create difficulties of administration and enforcement as it would be necessary to determine for each transmission which parts constitute a publication, a film or a game and to separately apply the relevant classification criteria to those separate parts. It might well be in a particular case that the text and pictorial matter is suitable for viewing by a minor (unrestricted publication), yet the document may include restricted or objectionable film and game material — resulting in up to three classification levels for the one on-line document. In such cases appropriate guidance may require an overall classification at the ‘highest’ level from among the constituent material — although variations in the ratings across the media may lead to confusion.

(iii) To deem on-line transmission to be a broadcasting service. This approach is attractive due to the developing convergence between telecommunications and broadcasting technology. Responsibility for broadcast regulation rests with the federal government, and this option has been successively examined by the Senate Committee and the ABA. Both bodies strongly supported limitations of the liability of network operators and computer service providers for the carriage of prohibited material, through defences based upon compliance with industry COP’s. While this approach is consistent with the strong reliance on self-regulation and enforcement through licencing provisions developed in the Broadcasting Services Act 1992, the reports diverge on the question of a broadcasting model for content censorship.

From this perspective, broadcast media are distinguished from publication by the absence of control over access to the material carried, and the Senate Committee held the view that on-line services are similarly unconstrained:

Clearly, some communications carried out via the Internet are one-to-one; for example, email and any encrypted messages (e.g. commercially sensitive matter). However, the Committee notes that the problem areas are open newsgroups and sites where objectionable material can be downloaded by thousands of people. Therefore, it considers that the difference between this process and conventional broadcasting is purely a matter of the technology used.

(Senate Committee 1995b para 54).

In the light of this conclusion, the Committee subsequently recommended the prohibition on-line of even low-level restricted material:

Recommendation 1: That it should be an offence to use a computer service to transmit, obtain possession of, demonstrate, advertise or request the transmission of material equivalent to the RC, R and X categories.

(Senate Committee 1995b page 18).

Yet there are inconsistencies in this approach. Presently, the effectiveness of broadcasting content censorship is due to commercial imperatives which do not apply to the general public. Further, the interactive nature of the Internet requires censorship of users as both source and target audience. In consequence, the Committee’s recommendation necessarily embodies some aspects of a publication-based model, yet imposes tighter restrictions than the existing OFLC scheme.

In contrast, the ABA has explicitly rejected a broadcasting model for on line services (ABA, 1996b), noting that “any legal definition of on-line services should be separate and distinct from any legal definition of broadcasting or broadcasting services. In this way the two will be dealt with according to their own particular characteristics”.

2.2.2 A New Classification Standard and Access Control
The development of a new classification standard specific for on-line transmissions as proposed by the ABA (1996b) again creates anomalies through differences in classification between the on-line and traditional expression of the same work. Of course, this approach introduces yet another level of classification criteria — criteria which are already complex and, at the margins, involve complex literary, scientific, artistic and social value judgments for which considerable skill and censorship experience are required. Yet its potential for simplification in the on-line environment may outweigh these objections, and the problem is then one of selecting an appropriate basis for development.

We have argued in the introduction that censorship levels should in many respects be determined by the level of control over inadvertent access. The problems of unsupervised access by minors to traditional broadcasting are self-evident, but their extent in the context of on-line services is a matter of some debate. In its earlier history, and even at present, there is little doubt that the Internet has suffered from these problems (albeit to a far lesser degree than radio and television) and some concern is warranted. Both the Senate Committee (1995b) and the ABA (1996b) have recommended that unrestricted Internet access be available only to clients over the age of eighteen (aside from exceptions for Universities) and that reasonable verification be undertaken by the service provider. Under such a regime, access by unsupervised minors becomes the responsibility of the adult account holder, and in relation to restricted material these responsibilities are markedly similar to those which currently apply when restricted material (magazine or video) is present in a residence occupied by minors. Consistency would therefore suggest that a generalised form of the publication model is an appropriate starting point for development.

We have noted in the previous section that an overarching publication model is more readily adaptable to ‘general’ on-line documents than other existing categories, and that it has already been judicially accepted as an appropriate model in on-line defamation cases. The approach is exemplified through the WA Censorship Act 1996 and the coverall definition of an article (s. 3):
AUSTRALIA APPROACHES TO INTERNET CONTENT REGULATION

“article” includes —
(a) a publication;
(b) a film;
(c) a computer program and associated data;
(d) a photograph;
(e) an object;
(f) a sound recording; and
(g) an advertisement for any article;

(together with separate computer service provisions so as to encompass on-line offences. This model is naturally applicable to the broadband services currently under consideration, as many may be regarded as digital articles — although one cannot rule out the emergence of services not readily covered through extensions to this definition.

However, responsibilities of Australian content providers under this model must be commensurate with those which presently apply to publication, and compulsory submission to the OFLC of all on-line material for classification is unworkable on the grounds of resources alone. It is apparent that pre-classification by the provider is the only reasonable solution, and this is discussed in Section 3.1.

2.2.3 Previous Statutory Prohibitions
Despite differences, there is some common ground between the various state laws concerning the types of conduct prohibited for restricted and objectionable material and there are natural analogies in an on-line context. Full details of these provisions may be found in Hogan and James (1996), but here a brief summary will suffice. Aside from “sale and hiring” and “production of objectionable material” offences, which require little explanation, the remainder may be grouped broadly as follows:

(i) “Public Visibility” Offences — whether the material is visible in a public place or left either in a public place or at private premises without the occupier’s consent — and “Attendance Offences” — whether a minor attends certain types of films or a parent or guardian allows them to attend. In an on-line framework, the relevant concepts concern inadvertent access to restricted material and allowing a minor to view such material.

(ii) “Possession and Copying” Offences — an adjunct to the “sale” offences, prohibiting the possession or copying of restricted material with the intention of selling or distributing. As in some drug offences, possession of multiple copies can be used as evidence of the intention to sell — and possession of RC material (especially child pornography) normally constitutes a very serious offence, irrespective of whether it is intended for sale or personal use.

While there is in principle no logical reason to distinguish between digital possession and physical possession offences, this does not adequately consider the nature of Web and BBS services and their underlying file transfers. In many respects, possession and sale have been generalised in the context of on-line services through the new offences of “downloading” or “requesting transmission” examined later.

(iii) “Tagging” Offences — whether the material bears the classification labelling appropriate to its content. In principle, these offences or a subset of them transfer directly to the on-line environment, but there are difficulties in ensuring that adequate information is provided to those who upload and may pre-classify such material. These issues are examined in Section 3.1.

2.2.4 Computer Service Provisions
As already mentioned several States and the Northern Territory are in various stages of enacting or implementing legislation to create new categories of offences relating to on-line services (Victoria and NSW) or computer services (Western Australian and Northern Territory). Whilst the definitions of these two services are similar, the on-line model incorporates a requirement of access being via the public telecommunications network, whereas that element is absent from the definition of “computer service”, possibly giving wider reach to include objectionable transmissions via a cable LAN.

The Western Australian and Northern Territory legislative models relate to the use of a “computer service”. Two categories of offences arise depending on whether the material is “objectionable material” or “restricted material”.

For “objectionable material” the offence in the WA Act (s.101) is to use a computer service to:

(a) transmit an article knowing it to be objectionable material;
(b) obtain possession of an article knowing it to be objectionable material;
(c) demonstrate an article knowing it to be objectionable material;
(d) advertise that objectionable material is available for transmission; or
(e) request the transmission of objectionable material knowing it to be objectionable material.

A defence exists for articles with recognised literary, artistic or scientific merit or bona fide medical articles but even in these cases, there must be a justification of the conduct based on it being for the public good.

For restricted material (s. 102) the offence is to “… use a computer service to transmit restricted material to a minor”, and various defences are provided. These include compliance with a COP approved by the relevant Minister (perhaps to be delegated in future to the ABA); taking reasonable steps to avoid the contravention; or a reasonable belief that the recipient was not a minor. Note that as the legislation stands the COP defence is not available to service providers in the case of objectionable material — a matter examined in Section 3.4.

In Victoria the offences relate to the use of an on-line information service to publish or transmit objectionable material — distinctions being made depending on the classification of the material and whether it is made available to a minor. Unlike the Northern Territory legislation, the Victorian model does not contain offences for obtaining possession of objectionable material or requesting transmission of objectionable
material (unless the material would constitute child pornography in breach of the “possession” provision in the Victorian Crimes Act 1958).

3 DISCUSSION
The release of the ABA Report and the subsequent abandonment of the NSW legislation have defused much of the controversy surrounding on-line regulation in Australia. While the report is in many respects an incremental development from the Authority’s Issues Paper (ABA, 1996a), the Inquiry substantially benefited from the emergence of the Platform for Internet Content Selection (PICS) (Resnick and Miller, 1996) extensions to the hyper-text transfer protocol — technology which will allow flexible and specific filtering of labelled Internet content.

PICS introduces a standard format for document labels independent of classification scheme, so that PICS-compliant browsers will allow users to disregard unlabelled material, and to select content classified according to the criteria of a ratings agency of their choice. In this fashion, browsers may be configured according to the differing needs of family members, and the Senate Committee concern over the absence of realistic controls over children’s access to ‘adult’ on-line material (Senate Committee 1995b) has now been substantially addressed.

The focus of Australian regulatory debates has now shifted toward the development of COPs acceptable to the ABA. While the ABA Report lists some features mandatory in an acceptable code, it remains silent upon more contentious issues such as the specific reporting requirements to be imposed upon computer professionals — and these issues are examined in Section 3.4.2. Of equal concern are unintended consequences of existing or proposed legislation, and issues such as encryption which have received inadequate attention, and these matters are considered below.

3.1 PICS and the Amateur Censor
The introduction of PICS compliant browsers will facilitate the addition of content labels to Internet materials. As noted above, a major virtue of the PICS standard lies in the ability of users to select the ratings system (and certifying agency) to be used for their account. Yet this flexibility raises two significant issues for Australian regulators: the extent to which Australian content providers will be required to pre-classify material; and the difficulty in ensuring that Australian censorship provisions are not effectively dictated by external classification agencies or regulatory authorities.

We have argued above on the grounds of consistency that the responsibilities of Australian on-line content providers should be commensurate with those which presently apply to publication. If such requirements are introduced, it is crucial that the OFLC be heavily involved in the development and dissemination of appropriate guidance through its Web page. Yet its resources are unlikely to permit the Office to act as a no-cost ratings agency for Australian material. While labelling of unrestricted material is desirable — and should be encouraged without sanction — the major legislative issue remains that of pre-classification at the restricted level, and there is an argument that tagging offences should be extended to this case. However, placement of the legal threshold for on-line material at the RC level (together with the likelihood that unlabelled material will be blocked out by family and school users) reduces the severity of such an offence and the matter becomes more of a discourtesy to other adult Internet users. In this light, a convincing argument may be made that the problem is better handled through ‘netiquette’-based notification to the account holder, and subsequently to his or her service provider.

The development of commercial and voluntary ratings agencies in the United States and elsewhere is likely to result in a de facto Internet censorship standard. While Australian users need not utilise particular ratings, Australian agencies may rely directly upon one or more such views when assessing overseas content, and so an official OFLC view of this material may be rendered irrelevant. The OFLC would greatly assist the Australian on-line community if it were to develop “equivalence tables” relating the criteria used by external agencies to the official Australian classifications. This information could then be used by service providers and local agencies — perhaps even through transparent conversion — to provide Australian users with guidance consistent across different media.

This discussion gives implicit support to the ABA’s proposal of a new online classification model (ABA, 1996b), yet also suggests the caveat that the model may itself become rapidly obsolete if it fails to take account of de facto standards as they emerge.

3.2 Knowledge and Inadvertent Access
While we accept the view of the ABA that the probability of inadvertently encountering contentious material is low (ABA, 1996b), we are concerned that inadequate attention has been given to the effect of the sophisticated Web and Usenet search facilities now linked to browsers such as Netscape. As some of these may provide limited descriptions of the matches found, it is in many cases quite reasonable for the user to examine the document before deciding whether it is relevant to the purpose of the search.6

Importantly, the WA legislative model incorporates an element of knowledge into the computer service offences (Section 2.2.4), so that users should not be liable for possession of the material until they have knowledge of its nature — an approach consistent with long-held principles of criminal responsibility. However, the ABA report is silent on this matter, and it is vital that the forthcoming legislative model incorporate provisions of this nature.

6 The situation described is particularly troublesome as the browser may cache material on disk without an explicit save command from the user. This would constitute notional possession and, if the material is examined sometime later by police, it may be difficult for the user to establish non-criminal intent or knowledge.
3.3 Difficulties due to Strong Encryption

The comments of the Senate Committee (see Section 2.2.1) discounting the importance of email and encryption in the transmission of contentious material are indicative of the failure of Australian regulators to address this issue. While embracing strong encryption, really authentication (Caeili, 1996), as the saviour of on-line enforcement (Recommendation 2, Senate Committee 1995b), the Senate Committee disregarded technical advice (Senate Committee, 1995a, 1995c) of the potential for frustration of enforcement by strong encryption algorithms, and of the likelihood that serious offenders would use this technology to go underground through email and private file transfer.

The use of strong encryption algorithms creates evidentiary difficulties for law enforcement agencies both in terms of detection of potentially offensive files when transmitted in an encrypted form and in their decryption prior to commencement of a prosecution. The existing court powers relating to ordering the decryption of material are far from certain. It would be desirable to ensure legislative backing were given to the power to order decryption to put the issue beyond doubt — in essence a stronger version of an existing Western Australian power (WA Act, s. 13) to order translation of contentious material into English.

Yet in the case of strongly encrypted material with lengthy keys, for symmetric ciphers 90 bits (Blaze et al, 1996), enforced decryption is dependent upon the co-operation of the offender or a prohibitively large investment in computing resources. Thus, in the absence of other evidence sufficient to convict, a careful offender may keep RC material outside the reach of the law, and avoid or limit liability on the pretense of a forgotten or misplaced key — leaving the judiciary to determine on some basis the veracity of these claims.

While these matters, as discussed in Hogan and James (1996), are noted in the ABA Report, there is no subsequent recommendation that the issue should be pursued further, and the omission remains a significant gap in an otherwise sophisticated regulatory framework.

3.4 Industry Codes of Practice

Under the ABA’s proposed regime, there are few aspects of the on-line service industry that will not be subject to the provisions of an approved COP. At the time of writing, it remains unclear whether a single industry-wide COP will emerge but some rationalisation seems both desirable and inevitable and the code developed for the Australian Internet Industry Association, presently in its second-draft (INTIAA, 1996) is likely to enjoy strong backing among ISPs. Much of this material is uncontroversial — especially that directed toward improving minimum standards of service from access providers — and need not be considered here. However, certain characteristics of “acceptable” COPs remain ill-defined, and must be examined in more detail.

3.4.1 Educational Responsibilities of Service Providers

No self-regulatory approach can succeed without adequate user education, and we concur with the ABA (1996b) that delivery of this material is best achieved through service providers — a matter incorporated into the INTIAA code (1996). In addition to elementary and PICS-related information, there is an undertaking (INTIAA, 1996) that the INTIAA administrative council will provide users with access to a Web page detailing authentication procedures and law relevant to Internet usage.

While this undertaking is welcome, it is imperative that legal information provided be current, and uniform across the industry, and we would argue that this is best achieved through a link to a federal government site. Hogan and James (1996) suggested that Web browsers sold or downloaded in Australia should display a warning message and link to such a page, and we reiterate this view.

3.4.2 Monitoring and Reporting Requirements

Successive federal inquiries (Senate Committee, 1995b; ABA 1996b) have recommended that industry COPs should include procedures to be followed by service providers in relation to the handling and blocking of illegal material and (where appropriate) referral to the relevant law enforcement agencies. While these bodies have accepted that ISPs have little or no knowledge of the material that may pass through or reside on their servers, there is an expectation that providers will actively investigate this material on the basis of reasonable suspicion or in response to complaints. These procedures lie at the heart of COP-based defences to computer service offences (Section 2.2.4), and the ABA has explicitly recommended that a code should not be registered unless it “... clearly details the conduct required that could constitute a defence” of the kind discussed.

The INTIAA draft code (1996) requires an ISP to remove RC-level material from a “Web site or other content database within its control” when it becomes aware of the presence of such material, and to warn or (upon repeated offences) cancel the account of the user concerned. These provisions are in principle adequate to deal with complaints in relation to accessible Web sites (although there is no requirement that the material be referred to law enforcement agencies), but the code does not yet address the more troublesome case of complaints involving a user’s private disk area. While privacy considerations do not apply to open Web sites, protected disk areas may contain confidential or commercially sensitive information, and users must also be protected from denial of service attacks through malicious complaints.

The coverage afforded by the definitions of the Telecommunications (Interception) Act 1979 is sufficiently broad that there are reasonable grounds to believe that viewing of email or transmitted files prior to receipt by the intended party constitutes unlawful interception under Section 7 of the Act — an indictable offence punishable by up to two years imprisonment. As this Act was drafted in the context of real-time communications, it is silent on the question of access to material after its receipt (such as examination of files on disk) and its potential application in this area is unclear. While it appears that this latter issue has not been judicially decided, examination of cases in relation to taping of telephone conversations (for example, R v Oliver
We believe that reporting requirements should be directed towards the detection and prosecution of serious offenders, while minimising prosecution of those who stumble upon illegal material. The INTIAA model may have some advantages in the latter case, but as noted in Section 3.3, serious trafficking in RC material is likely to take place through private encrypted email and file transfer, and the discussion above highlights a number of problems facing ISPs should they be required to investigate complaints of this nature.

Noting these difficulties, and the potential cost in staff time to diligent providers, it is our view that complaints in regard to illegal on-line material within Australia should be forwarded directly to the OFLC or police forces, and that examination of user areas should be undertaken only in conjunction with properly authorised law enforcement officers. The ABA (1996b) has indicated support for a nationally publicised email address for reports of available RC material, and it would be straightforward for the industry to develop a standard complaint interface to such an account. Similar referrals could be made if ISP staff encounter suspect material in their normal activities, but contractual protection against civil action by an aggrieved user must be provided in such cases, and this is yet to be addressed in the INTIAA code.

3.4.3 COP Defences and Knowing Possession

The code of practice defences discussed above are based upon recognition by regulators that ISPs will normally be unaware of the content of material passing through their servers. It is inconsistent, therefore, that the WA computer service provisions allow a COP defence in relation to carriage of restricted material, but exclude it in the case of objectionable material. While the offences rightly require an element of knowledge, the special status of service providers should be acknowledged through amendments to this legislation.

In the light of such inconsistencies, some caution must be exercised by those responsible for development of COPs, and those intending to report suspected RC material. For example, section 7.6 of the INTIAA draft code (1996) requires ISPs to make reasonable efforts to inform the owner or controller of a site containing RC-level material of its existence — in some circumstances an admission that ISP staff have knowingly possessed (and/or knowingly requested) the transmission of RC-level material. While the staff may have correctly followed the relevant COP procedures, the defence may not be available and criminal liability may apply.

4 CONCLUSIONS

The framework for on-line services which has emerged following the ABA Report is a sophisticated approach to the regulatory challenges posed by the technology, and is far less prescriptive than had previously been feared. However, the responsibilities of computer professionals under industry codes of practice remain unclear in some important respects, and no government body has yet adequately addressed issues of strong encryption in the context of trafficking of RC material. It is imperative that organisations such as the Australian Computer Society and the Systems Administrators Guild of Australia be actively involved in the initial and ongoing development of COPs, so that ISP staff are not placed in situations which may be ethically or legally compromising.

ACKNOWLEDGEMENTS

The authors would like to acknowledge helpful discussions with Professor Bill Caelli, research assistance from Chelsea Evans and Ben Zillman, and very useful suggestions from the referees.

REFERENCES


BIографical notes

James M Hogan lectures in Computer Science at the Queensland University of Technology. His main areas of interest are randomly connected neural networks, knowledge representation, and information technology law.

Peter Cl James is a partner in the Brisbane office of the law firm Allen, Allen, and Hemsley, and practices primarily in information technology law.
Copyright in Shareware Programs Distributed on the Internet

Cristina Cifuentes
Centre for Software Maintenance, Department of Computer Science, The University of Queensland, Brisbane, Queensland 4072 cristina@cs.uq.edu.au

Anne Fitzgerald
School of Law, University of Tasmania, Hobart, Tasmania 7001 anne.fitzgerald@law.utas.edu.au

The intellectual property of software developers has been protected by copyright since amendments to the Australian Copyright Act in 1984. In the first Australian case to consider copyright in a shareware program distributed on the Internet, the Court held that the Internet service provider OzEmail had infringed Trumpet Software’s copyright in Trumpet Winsock 2.0B by arranging for the program and a set of altered data files to be distributed with other software on diskette as a give-away inserted in copies of computer magazines. The implications of this case for software developers, distributors and users are discussed.

Keywords: copyright, shareware, computer software protection, licence, implied licence

1 INTRODUCTION

Many software companies are now using the Internet to distribute their products and the proportion of software sold on the Internet rather than in the form of shrink-wrapped disks can be expected to continue to increase. Internet distribution is particularly suitable for smaller or cheaper programs or those which are frequently upgraded. Probably the best known example of Internet software distribution is Netscape Navigator, the beta version of which was distributed free on-line, enabling it to rapidly achieve its position as the leading web-browser software.

Much of the software distributed on the Internet is currently marketed as shareware, allowing potential purchasers to test it for a specified evaluation period before registering it. The distinguishing feature of shareware, as opposed to freeware and public domain software, is that it is distributed on a “try before you buy basis”. Whereas the conventional means of software marketing requires users to purchase a shrink-wrapped and untried diskette, shareware marketing makes the software available to users without charge for the purpose of evaluating it before purchase. Those who want to continue using the software at the expiration of the evaluation period (usually 30 days) must pay a registration fee to the owner. The success of shareware has been largely dependent on the expectation that at least a proportion of users will be honest enough to pay the registration fee. More recently, a degree of practical protection has been incorporated into shareware distributed on the Internet in the form of a time-lock which renders the program unusable unless registration has been effected.

This paper presents and discusses a recent case involving a shareware program distributed on the Internet, Trumpet Winsock 2.0B, which was distributed on diskette in a modified form by OzEmail, an Internet Service Provider (ISP), without the permission of the copyright owners. The paper is structured in the following way: the origins of the shareware method of distribution are described in Section 2, Section 3 summarises the protection afforded by computer programs under Australian copyright law, Section 4 explains the normal use of the Trumpet Winsock program, Section 5 explains the use of the software by OzEmail, Section 6 presents the judge’s conclusions, and Section 7 discusses the implications of this case for the computing community, and particularly ISPs and software owners.

2 THE NATURE OF SHAREWARE SOFTWARE

The concept of shareware software originated in 1982 with two independent software developers, Jim Knopf and Andrew Fluegelman. They distributed their respective software, PC-File and PC-talk, with a message in the program asking those who received it to voluntarily send a modest donation ($10 and $25 respectively) to the author (Knopf, 1987). Knopf used this method to help defray the cost of distribution of new versions of the software (basically upgrades and bug fixes) to his mailing list of users, while Fluegelman used this method as a new marketing experiment. Both authors decided to...
collaborate on this new concept and the success of shareware followed. The immediate success of shareware has been attributed to various factors, including: the availability of the first IBM personal computers (PCs) and the need for users to obtain software to run on this new computer, the high price of other software, the absence of any trial period with commercial shrink-wrapped software which would enable users to decide whether the software is useful to them, and the need of computer club librarians to share programs with their members.

In April 1987, a small group of software authors and vendors formed the Association of Shareware Professionals (ASP), with Jim Knopf as its first Chairman. The aim of the founders of this not-for-profit association was to strengthen the place of shareware as an alternative to commercial software and encourage a broader distribution of software. Shareware was defined then as “try before you buy”. The ASP has grown into a large organisation, with members including software authors, publishers, shareware vendors and electronic bulletin board system operators (BBSs).

Shareware programs were very popular in BBSs, which provided a good distribution method for software authors. They were also made available by computer shops and clubs which would charge a nominal fee (normally between $3 to $10 dollars) for a copy of the software. However, with the increased usage of the Internet, shareware authors now distribute their software on ftp sites worldwide, which offers the advantage of a potentially much wider distribution. There are several well-known shareware sites on the Internet, including SimTel, Garbo, Jumbo and CICA. These sites distribute shareware software in the form provided by the author of the software for different types of computer and different operating systems, with Windows 3.x being the category for which the largest number of shareware programs is available. The recent expansion of the World Wide Web and the development of more sophisticated search engines has made it much easier for users to find software they are interested in. Most shareware sites include search engines and lists of the software available at that site.

Shareware software is now very popular and users can find the software they need at a price that suits them. Many acknowledge that most shareware programs are of good quality and are relatively inexpensive for the functionality provided (Needleman, 1992). One of the problems with this distribution method is that it is based on an honour system whereby it is up to the user to register the software if it is useful. Therefore, different methods have been used by authors as an incentive for shareware users to pay the registration fee. Some of these are: a trial period (usually 30 days), availability of printed documentation for the program, availability of the full version of the program, and time-lock expiry of the program after installation.

3 COPYRIGHT PROTECTION FOR COMPUTER SOFTWARE

Computer programs have been protected by copyright as literary works since amendments to the Copyright Act in 1984. Section 10(1) of the Copyright Amendment Act 1984 defines “literary works” as including “a computer program or compilation of computer programs”. A “computer program” is defined as:

"an expression, in any language, code or notation, of a set of instructions (whether with or without related information) intended, either directly or after either or both of the following:
(a) conversion to another language, code or notation;
(b) reproduction in a different material form, to cause a device having digital information processing capabilities to perform a particular function”.

The recent High Court decision in Autodesk v Dyason (No 1) (Autodesk v Dyason, 22 IPR 163, 1992) made it clear that copyright protection for computer programs is not limited to the written source code but also covers the object code stored on a disk, ROM or EPROM.

The owner of copyright in a computer program enjoys the same economic rights as are provided for other literary works in Section 31(1)(a) of the Copyright Act. The owner of copyright has the exclusive right to:

(a) reproduce the work in a material form;
(b) publish the work;
(c) perform the work in public;
(d) broadcast the work;
(e) cause the work to be transmitted to subscribers to a diffusion service;
(f) make an adaptation of the work; and
(g) do any of the acts (a) to (e) in relation to a work which is an adaptation of the work.

Following recent amendments to the Copyright Act, Section 31(1)(d) also provides the owner of copyright in a computer program with the exclusive right to control the commercial rental of the program. Copyright is infringed when someone does or authorises the doing of one of the acts included in the copyright owner’s bundle of exclusive rights, without the permission of the copyright owner, whether in relation to the entire work or a substantial part of it.

The Copyright Act does not define what constitutes a reproduction of a work, although “material form” is defined as including, “any form (visible or not) of storage from which the work … or a substantial part of the work …, can be reproduced”. The words “visible or not” were introduced to cater for object code, as object code cannot be read in the same way as source code or any other literary work is read by the human eye. Hence, reproduction in a material form includes reproduction in any form of storage, including a (non-visible) digital form, from which the work or a substantial part of it can be reproduced.

It is apparent that in the case of software, almost every use will constitute a reproduction which will infringe copyright; it is a reproduction of a computer program to copy the program onto a disk or onto the hard drive of a computer. In its Final
Report on Computer Software Protection (1995), the Copyright Law Review Committee (CLRC) also regarded the reproduction right as arguably being exercised whenever a computer program is used, since running the program in a computer normally involves the intermediate reproduction of the program in the computer's RAM. The CLRC recommended that such intermediate reproduction of a program should be an exception to the owner's exclusive rights.

"Adaptation" is given a special meaning in relation to computer programs. Section 10(1) provides that "adaptation" means

"(ba) in relation to a literary work being a computer program — a version of the work (whether or not in the language, code or notation in which the work was originally expressed) not being a reproduction of the work;"

Finally, a licence arises when the copyright owner gives permission to another to do an act which would otherwise constitute an infringement (Lahore, 1988). Copyright licences may be granted expressly or arise by implication, and, unless the licence is an exclusive one, there is no need for it to be in writing. A licence may be implied from the circumstances in which the owner deals with the work or from the custom of the trade; although a licence will only be implied where business efficacy demands it (McKeough and Stewart, 1991).

4 THE TRUMPET WINSOCK PROGRAM

Trumpet Winsock is a Windows TCP/IP networking communications program for the PC that allows a computer to connect to another computer, whether for example a bulletin board system or an ISP, using Windows sockets.

Trumpet Winsock was written by Peter Tattam who for ten years up to September 1994 worked as a computer programmer in the Psychology Department of the University of Tasmania. The program was written by Mr Tattam independently of his employment with the University of Tasmania and copyright in it is jointly owned by Mr Tattam and Trumpet Software Pty Ltd (Trumpet), a company founded by him and of which he is Managing Director. Version 1.0A of Trumpet Winsock was released on 1 February 1994 and it rapidly gained an international reputation as the best available software for connecting with the Internet. Guidelines to the Internet published during 1994 and 1995 invariably advised readers to use Trumpet Winsock for Internet connection (Levine and Levine Young, 1994; MacBride, 1995; Goodheart and Crawford, 1995; Ebbs and Horey, 1995). Trumpet Winsock has been distributed in shareware mode and has been used world-wide for connection to the Internet and local universities.

The Trumpet v OzEmail case concerned version 2.0B of the software which was released by Trumpet in 1995 and was distributed on the Internet as shareware through various means such as BBSs and ftp sites; including Trumpet’s site and that at the University of Tasmania. Version 2.0B was distributed in zipped format. The unzipped file consisted of 15 files; an additional file, trumpwsk.ini, was generated when the Trumpet Winsock program was first run. The 15 files and sizes in bytes are:

- readme.msg: 318 bytes
- disclaim.txt: 640 bytes
- install.doc: 66,048 bytes
- install.txt: 35,132 bytes
- winpckt.com: 3,516 bytes
- winsock.dll: 145,152 bytes
- tcpman.exe: 119,040 bytes
- sendreg.exe: 39,168 bytes
- pingw.exe: 26,112 bytes
- services: 2,840 bytes
- protocol: 441 bytes
- hosts: 96 bytes
- login.cmd: 1,901 bytes
- bye.cmd: 65 bytes
- setup.cmd: 271 bytes

As can be seen, this distribution of the software did not contain an installation program, hence a user would normally have to read the readme.msg and/or install.txt (or its Word equivalent install.doc) file(s). The former file tells the user that the Trumpet Winsock software is distributed in shareware mode and that the documentation is in the install.txt (or install.doc) file. The introduction section of the 42-page documentation file informs users that the product has been released as shareware and that it has an evaluation period of 30 days. It requests a registration fee of US$25 if the user finds the software of use, to enable the continued development and support of the software. The documentation then explains to the user how to install the Trumpet Winsock program and how to run it. It also explains the usage of the scripting language which allows users to create a login script to directly connect to a computer. The documentation points out that many ISPs have written their own scripts for connecting to their site and a sample file is provided with the distribution (login.cmd).

When the program is first run, a setup screen is displayed asking the user for configuration information details to enable the TCP/IP package. This information is stored in the newly-created trumpwsk.ini file. Figure 1 shows the window normally displayed by the software. As can be seen from the figure, the copyright and shareware notices are displayed in this window. The program then connects the user to the Internet address previously specified (and stored in trumpwsk.ini).

![Figure 1: Trumpet Winsock Opening Screen.](image-url)
The documentation ends with information on how to register the program. By registering, a user receives a password and a user name which replaces the UNREGISTERED VERSION notice on the main window (see Figure 1). Technical support is also available to registered users, as well as upgrades within the following 12 months. This version of the software has a Send Registration option available on the File menu to automatically register a user by sending the credit card details in an encrypted way when the user is connected to the Internet. This option is executed by running the sendreg.exe program. Both user and multiuser licences of the software are available. The last page of the documentation states that should a user want to distribute Trumpet Winsock with other programs, a suitable offer should be made to Trumpet for their consideration.

5 THE TRUMPET V OZEMAIL CASE

OzEmail is an Australian-based ISP that provides commercial access to the Internet. It is Australia's largest ISP, with an estimated 82,000 active customers as at 30 June 1996, and recently listed on the Nasdaq stock exchange.

In late 1994, Trumpet was approached by the Managing Director of OzEmail Pty Ltd (OzEmail), Mr Sean Howard, with proposals to distribute Trumpet Winsock on diskette in an upcoming edition of Australian Personal Computer (APC) magazine, and to include Trumpet Winsock on a software package diskette to be distributed by OzEmail at a retail price of Au$50. There was no further contact until 8 March 1995 when Mr Tattam received a fax from OzEmail's Project Manager, Mr Urquhart, requesting confirmation of OzEmail's understanding that they could freely distribute approximately 60,000 copies of Trumpet Winsock 2.0B on the cover of the April 1995 edition of the APC magazine, at no commercial gain to OzEmail. On 10 March 1995, Mr Tattam informed Mr Urquhart that he did not want OzEmail to proceed with the distribution because Trumpet Winsock 2.0B was not timelocked and he was concerned that the distribution proposed by OzEmail would result in many people using the software without paying the registration fee. At that time, Mr Tattam was working on the timelocked version, which eventually was released as Trumpet Winsock 2.1, and therefore he agreed to the distribution of the timelocked version in the magazine, once he had finished writing and testing it.

Dissatisfaction in his dealings with OzEmail during the following couple of weeks led Mr Tattam to decide to terminate all negotiations with them regarding distribution of Trumpet software. He wrote a letter to OzEmail informing them of this decision on 3 April. Unknown to Mr Tattam, at this time OzEmail had already distributed Trumpet Winsock 2.0B on diskette in about 60,000 copies of the April 1995 issue of APC. The Trumpet Winsock software used by OzEmail for this distribution was the unlocked version, 2.0B, which they had downloaded from the University of Tasmania's ftp site. The software (along with other freeware software) was also made available at OzEmail's ftp site.

OzEmail's distribution of Trumpet Winsock 2.0B had some modified and additional files in order to allow users to directly connect to their site. These changes were made to help users connect to the ISP and to simplify the process of installing the software as most non-computing users would find it hard to understand the 42-page installation document.

The changes included:

(i) The script file login.cmd was modified to directly connect to OzEmail. In its original form, the login.cmd file did not direct the user to any specific ISP.

(ii) A trumpwsk.ini file was supplied to connect the user to OzEmail. This file was normally generated by running the program for the first time.

(iii) The script file bye.cmd which disconnects the modem was modified (a bug was actually introduced).

However, OzEmail's distribution omitted several important files which informed users that the Trumpet Winsock software is shareware. Two files — readme.msg and install.txt — were deleted completely. The install.doc file was renamed to trumpet.doc and a WriteNow icon was made available to load this documentation file; resulting in garbled information on the user's screen as the file was in Word format. The deletion of these files counteracted the normal installation process for Trumpet Winsock. As previously noted, a user would normally read the readme.msg and/or install.txt (or equivalent install.doc) file in order to install the software. In OzEmail's distribution, these steps could not be followed as the software was modified by means of its data file. Further, its documentation and registration files were missing. Overall, to a user that installed this distribution, the only reference to the shareware nature of this software was that in the opening window of the program (Figure 1), but should a user want to know more about the shareware nature of the software, the documentation was not readily available.

The effect of the various additions, deletions and alterations to the software was that the user would connect directly to the OzEmail network. These changes also deleted or obscured the messages in Trumpet Winsock 2.0B which informed users that the software was shareware distributed for evaluation purposes only and the details of how to register with Trumpet. As a result of these changes, the user was left without any clear instructions that Trumpet Winsock was shareware or the need to register at the end of the 30-day evaluation period.

In May 1995, Trumpet's solicitors wrote to OzEmail asserting that OzEmail's actions in reproducing Trumpet Winsock 2.0B, and in distributing the modified version of it, infringed Trumpet's copyright and contravened the Trade Practices Act 1974. Despite protests from Trumpet through their solicitors, OzEmail again distributed copies of the modified Trumpet Winsock 2.0B program on another 60,000 diskettes included in a second magazine, Australian PC World, in August 1995.
6 THE FEDERAL COURT'S DECISION

Heerey J held that OzEmail had infringed the copyright of Trumpet and Mr Tattam in Trumpet Winsock 2.0B and had contravened the provisions of Part V of the Trade Practices Act 1974.

6.1 Copyright infringement

It was not disputed that the compilation of files making up Trumpet Winsock together constituted a computer program which attracted copyright protection under the Copyright Act 1968, or that copyright was jointly owned by Trumpet and Mr Tattam.

As explained in Section 3, computer programs are protected as literary works under the Copyright Act 1968, attracting the same economic rights as apply to other literary works. Of the several exclusive rights listed in Section 31(1)(a) of the Act, the only one considered by the court was the right "to reproduce the work in a material form". Heerey J found that OzEmail had reproduced or authorised the reproduction of a substantial part of Trumpet Winsock in two ways: by downloading the program from the University of Tasmania's ftp site and reproducing it on OzEmail's ftp site, and by making or authorising the reproduction of Trumpet Winsock on diskettes distributed in Australian PC and Australian PC World. This much was not in dispute, having been admitted by OzEmail in their pleadings.

The issue thus was whether OzEmail had, as it claimed, the licence and consent of Trumpet to deal with Trumpet Winsock in this way. Specifically, the questions addressed by Heerey J were whether any licence which Trumpet may have given to OzEmail to publish the software had been revoked and, if not, whether OzEmail had breached the conditions of its licence.

Heerey J held that any licence which OzEmail may have had to use Trumpet Winsock was revoked in the conversation between Mr Tattam and Mr Urquhart on 10 March 1995. During that conversation, which occurred prior to the first distribution on the APC magazine, Mr Tattam expressly told OzEmail that he objected to them using the unlocked version of the software for the proposed distribution in APC, OzEmail argued that a licence to do the acts it had done could be inferred from the fact that Trumpet had widely published and distributed the software around the world, described as shareware, free of charge and with no restriction imposed on the use or distribution of the files, except when offered or distributed for sale.

However, Trumpet argued that if the fact that the software was distributed as shareware on the Internet gave rise to an implied licence to intermediaries to distribute the program to third parties, then that licence was subject to the conditions that such distribution should be:

(i) without other software;
(ii) without modification, addition or deletion;
(iii) in its entirety; and
(iv) without charge and not for commercial gain;

to enable third parties to use the software for 30 days for evaluation purposes.

In ascertaining any implied terms which are to be included in a shareware licence, Heerey J relied by analogy on the doctrine of implied contractual terms expounded by the Privy Council in BP Refinery (Westernport) Pty Ltd v Shire of Hastings (BP Refinery, ISO CLR 266, 1977). Two of the BP Westernport criteria which were seen as particularly relevant were:

(a) whether the supposed condition is necessary to give business efficacy in the light of the fundamental purpose of shareware; and
(b) whether it is so obvious that it "goes without saying".

On the basis of evidence from computer experts regarding the nature of the terms and conditions of shareware licensing, it was found that industry practice, while not establishing custom in the legal sense, did support conditions (ii) and (iii) above. Applying the BP Westernport criteria, Heerey J concluded that

"... it is essential, that in the case of a distributor dealing with shareware, it be distributed in its entirety and without modification, addition or deletion. The whole purpose of evaluation is to enable the end user to evaluate the product as produced by the author." [emphasis in original]

However, the court rejected Trumpet's submission that the licence also included terms that the software was not to be distributed with, or accompanied by, any other software; although this was mentioned in the last page of the documentation file. Provided the accompanying software was sufficiently separately identified and did not interfere with the operation of Trumpet Winsock, the fact that it was distributed with other complementary Internet software was no ground for objection. The court also rejected Trumpet's submission that a condition be implied that the distributor could not make any charge or commercial gain. The possibility of making a profit provided an incentive to the distributor to deal with the
shareware and this additional distribution should benefit the software owners. The amount of profit could not be limited to a "small" or "modest" one, but would be determined by market forces.

Heerey J concluded that even if any licence in favour of OzEmail had not been revoked by Trumpet, OzEmail had breached conditions of the licence by the changes it made to Trumpet Winsock 2.0B. The changes which OzEmail made to Trumpet Winsock without Trumpet’s permission were significant and would have an adverse impact on Trumpet’s commercial interests, as they could damage Trumpet’s position as an independent marketer of software for Internet access and its commercial relationship with other ISPs. Also, the notification of Trumpet’s rights to payment from users who decided to keep the software were seriously obscured. OzEmail’s purpose in distributing Trumpet Winsock was not the evaluation of the program for its own use or distribution to other users for evaluation, but to use it as a free give-away to attract subscribers to its own ISP service.

6.2 Trade Practices Act

Heerey J also held that OzEmail infringed Section 52 of the Trade Practices Act 1975, which provides:

“A corporation shall not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive.”

Firstly, as purchasers or readers of the two computer magazines would assume that the distribution of the diskettes containing the software took place as a result of some arrangement or connection between Trumpet and OzEmail, they would be mislead or deceived into believing that OzEmail had the permission, licence or authority of Trumpet to publish the software. Secondly, OzEmail’s conduct would be likely to mislead or deceive readers of the computer magazine and users of the programs on the diskette into believing that it was not necessary to obtain a licence from Trumpet to use the software. A number of factors combined to create this impression: the reference in OzEmail’s brochures to “free software”, the fact that Trumpet’s shareware message was obscured, and the emphasis on the registration fee of $25 payable to OzEmail while failing to make it clear that a fee of the same amount was required to be paid to Trumpet.

7 DISCUSSION AND CONCLUSIONS

As the first Australian case dealing with copyright in a computer program marketed as shareware on the Internet, the decision in Trumpet v OzEmail is an important one. It has implications both for owners of software distributed on the Internet and for ISPs and others who distribute it.

Heerey J’s judgment makes it clear that copyright continues to subsist in computer programs distributed as shareware on the Internet. By using this form of marketing, the owners do not somehow “lose” or impliedly abandon copyright in their software, donating it to the public domain for anyone to reproduce, distribute and use as they please. Subject to any express or implied licence conditions, the owners of copyright in software distributed as shareware continue to enjoy the exclusive rights accorded by the Copyright Act 1968.

As the Internet has developed, it has been recognised that it may be necessary to imply licences to permit certain uses of works which would otherwise infringe copyright. This is the first case in which a court has considered the kinds of implied licences which will apply to copyright materials distributed on the Internet. On the facts of this case, a licence was implied based on Trumpet Winsock’s distribution as shareware, which provides for the distribution of the software “in its entirety and without modification, addition or deletion”. However, it was not considered reasonable to qualify the licence as urged by Trumpet, i.e., that any distribution by an intermediary should not be accompanied by other software or that the distributor should not be able to make a charge or commercial gain.

Unlike copyright materials which are embodied in tangible media, works put onto the Internet can readily be copied and re-distributed and are effectively out of the copyright owner’s control. Owners of software distributed on the Internet need to make it clear to users that it is protected by copyright and set out the terms on which it can be copied, used and re-distributed. In the light of the Trumpet decision, if software developers distributing their work as shareware on the Internet require users to obtain a licence for the distribution of an entire, unmodified version of the software on a commercial basis or accompanied by other software, they will need to expressly state this in the shareware licence.

Following the decision in Trumpet v OzEmail, ISPs and other distributors of shareware programs will have to exercise more care when dealing with software. Many ISPs have provided new users with diskettes containing selected Internet connection software such as Trumpet Winsock. Often, they change the communications software included in their distribution by adding, deleting and modifying files in the shareware for the purpose of enabling direct connection to the ISP. These changes also have the effect of obscuring or removing information about the shareware nature of the program, copyright ownership and disclaimer of liability. The effect of the court’s decision is that ISPs cannot make such changes without the express permission of the copyright owner. In the absence of an express licence to distribute the shareware program in a modified form, one will not be implied and shareware which is distributed as part of an Internet connection package must be in its entirety, without modifications, additions or deletions.

REFERENCES


CALL FOR PAPERS

Software Quality Conference

The Software Quality Association (NSW) is organising an international conference on software quality to be held in October 1997. The aims of the conference are to promote co-operation and greater understanding among both academics and practitioners by providing an opportunity to share research and practical experience.

Submissions for the conference are now invited from both practitioner and academic authors. Two kinds of submission will be considered:

- Formal papers which may be theoretical, conceptual, tutorial or descriptive in nature and which must not have been previously presented or published;
- Industry presentations which may present case studies or practical experience.

Formal papers should include a title page and an abstract on separate pages. The title page should include the title of the paper, full names of authors, affiliations, and complete addresses, telephone numbers, fax numbers and e-mail addresses (if available). The abstract should be a minimum of 300 words and the complete paper between 10 and 15 single-spaced pages including references and figures.

Industry presentations should include a title page, a two page management summary and a set of the presenter's visual materials. The title page should include the title of the paper, full names of authors, affiliations, and complete addresses, telephone numbers, fax numbers and e-mail addresses (if available).

One copy of a one page summary is required by 18 April 1997. Three copies of the final paper or presentation are required by 30 June 1997 to facilitate peer review. Notification of acceptance will be mailed to the first author on or before 6 August 1997. For inclusion in the Conference Proceedings, completed papers must be received on computer disk by 6 September 1997. Conference Proceedings will be distributed at the conference.

CONFERENCE TOPICS

Submissions are invited on all topics related to software quality, including but not limited to:

- Quality Management Systems
- Standards and Certification
- Process Improvement
- Product Standards and Certification
- Metrics and Measurement
- Year 2000 Quality Strategies
- Change Management
- Configuration Management
- Reviews and Audits
- Testing and Evaluation
- Validation and Verification
- Risk Management

Submissions based on practical experience are particularly welcome.

Please send formal papers to:
David Wilson
School of Computing Sciences
University of Technology, Sydney
PO Box 123, Broadway NSW 2007 Australia
Tel: +61-2-9514 1832
Fax: +61-2-9514 1807
e-mail: davidw@socs.uts.edu.au

Please send industry presentations to:
Alan Williams
SQA Conference
PO Box 411, Carlingford NSW 2118 Australia
Tel: +61-2-9378 5924
Fax: +61-2-9378 5945
Internet Ethics’ Bibliography

This Bibliography has been collected, recompiled and selected by Porfirio Barroso Asenjo

**BOOKS**


**BOOKS’ CHAPTERS**


**JOURNALS**


Reading Tonya’s e-mail. (1994): (Reading Tonya Harding’s e-mail) (includes a list of ethical codes for journalists using e-mail sources). In: American Journalism Review, April, 16(3):12.


**MAGAZINES**


INTERNET ETHICS BIBLIOGRAPHY


Net censors. (1996): (CompuServe is developing software that will block access to certain sexually-explicit Internet sites on a country-by-country basis) (Brief Article). In: Maclean's, January 15, 109(3):45.


STERN, C. (1996): CompuServe shuts down sex after German protest; online service blocks access to Internet sites. (Sex-related Internet sites) (In: Broadcasting & Cable, January 8, 126(2):69.


NEWSPAPERS


THE AUSTRALIAN COMPUTER JOURNAL, VOL. 29, NO 1, FEBRUARY 1997
INTERNET ETHICS BIBLIOGRAPHY

HOLCOMB, T. (1995): A
Thursday, January 26:B1 (W), B1 (E).
MAGID, L.J. (1994): Users can get religion on-line. (Online services that address religious and ethical issues). In: San Jose Mercury News, November 27:1E.
NATIONAL EMBARGO: Wires from the Garbage Heap. In: Los Angeles Times, Saturday, February 27:IE.
NEW YORK TIMES, Monday, October 9:D4.
NEWSPAPER ON-TO-ON: Slander. In: Los Angeles Times, Sunday, March 10, (899?):1.10.
SLURS POSTED ON INTERNET RAISE CENSORSHIP QUESTIONS; NETWORK LETS USERS REACH MILLIONS. BUT WHAT IF MESSAGES ARE SLANDEROUS OR DECEITFUL? In: San Jose Mercury News, May 1:1D.
In fact modem graphical interfaces have even made using the Web a pleasure. Exchange to the global wealth of information it represents today, the Internet eyes. From humble beginnings in the AARNET for academic information such as gif, jpeg and html. A quick click of the mouse and the document is easily printed. Of course, one cannot actually edit or modify the document, except by opening it from a relevant application.

More than this, QuickView Plus makes itself very convenient to use by integrating seamlessly with the Windows Explorer (so any file may be easily viewed by the right mouse button menu), the Windows '95 File Find (so found files may be viewed), Microsoft Exchange (so email attachments may be easily viewed), and a number of other applications, such as Netscape (as the default helper application for unrecongised file types).

It really is highly useful — in fact, it is almost unbelievably useful, just as its advertising blurb declares. Certainly it has found a permanent spot on my bookshelf. In some ways, one could evencept that is referred to repeatedly.

QuickView Plus is available in both Windows 3.1 and Windows '95 incarnations, as well in single user and LAN versions.

David Williams
Quality Coal Consulting


This is a very refreshing book on C programming, with the added benefit of being authored by an Australian academic. In particular, it is not another in the plethora of C texts, rather it is specifically aimed at students with a strong programming background and at professional programmers (from the preface, p. ix). It covers the concepts of programming with C (variables, scope, rvalues, lvalues, character stream I/O and so forth), advancing onto the concepts of ANSI C and concluding with a very useful section on Unix systems programming. All topics are covered with considerable depth and in an most accessible manner, with many examples, diagrams and revision questions.

Throughout the book the importance of C concepts are related to both applications and systems programming. The particular distinctive of C is emphasised through a virtual machine concept that is referred to repeatedly.

A comment must be made on grammar and spelling — unfortunately, one will quite quickly come across many errors. However, if one can be tolerant of such, I do believe this book to fill a particular niche well. It certainly has a one page summary at the end of each chapter entitled: for the Time reader who must plod from page one all the way through and then start typing. The author asks us What will make them visit again?

Try your own University’s page. Curiosity will bring a visitor to your page and the author asks us What will make them visit again?

Pfaffenberger has advice on how to publicise the fact that you now have a home page up and awaiting visitors. This is useful point to keep in mind. I know of an organisation that insists it has a Web presence but I am dammed if I can find it. A page is an advertisement and an advertisement is no good at all if it does not have an audience.

Part I starts us off with a quick introduction to the Internet and then a few chapters on understanding the terms used (eg HTTP — HyperText Transfer Protocol — hypertext is a form of non-sequential writing championed by Ted Nelson in 1965; URL — Uniform Resource Locators; HTML — HyperText Markup Language). These are important chapters because they give us an overview of the Web and its differences, mainly that the Web is interactive and distributed. The author highlights the fact that in Web publishing, the reader chooses which bit to read next (hence HyperText — which has its roots in Hyper Space). The reader can jump from one spot to another willy nilly as their mood dictates unlike a book which is read sequentially from front to back (with due apologies to the Chinese and Arabs who read the other way). Writing for a HyperText cogniscent audience is, apparently, vastly different from writing normal prose.

Part II — chapters 6 to 9 — tells us how to design our site. We are taught how to choose the appropriate server, how to develop a publishing plan with emphasis on our purpose. There is an important chapter on the do’s and don’ts of Web publishing.

Part III is the meaty bit. From chapter 10 through to 20 we are taught how to physically do the creating of our Web site. We are taught how to create a HTML document, how to build a document, how to add hyperlinks and multimedia and how to get user feedback.

Part IV is for the advanced Web user and teaches us how to use multimedia in our Web sites. Part V is entitled Web Publishing Issues and is rather enlightening in regards to Security, Copyright, and Standardisation.

Up at the back of the book is a CD ROM with all the software you will need to start your page and get it up and running. It includes a HTML editor, 1,000 pieces of clipart, 200 sound bites and several other Web tools. All very useful.

Pfaffenberger caters for the three types of reader. You know, there’s the reader who must plod from page one all the way through and then start typing. They can easily do that with this book, it is not boring. Then there is the reader who is in a bit of a hurry and wants more of an ongoing tutorial. The author has a one page summary at the end of each chapter entitled: for the Time challenged. And for the reader who insists on typing straight away — well just go straight to chapter ten and off you go!

I have no trouble in recommending this book to those who are thinking of creating a Web site. It will teach you how to do it, surely, but the book is much much much more than lesson in how to create a home page. It teaches how to make a good or even a great homepage.

The book is good, too, for those who are just curious about how it all happens. The book has an easy to read style that will not bore those who want a tutorial or those who want an overview.

Pfaffenberger has done a great job in presenting a complex task in simple English. He gives us the why, the what, and the how.
This book provides a helicopter view on many computer technology related issues ranging from Artificial Intelligence to Teacher Education around the world. It examines a wealth of topics in computer education but rarely goes further than an overview of the topic. The educator who wants an in-depth study of a particular field should look further than this book. It would be better suited to a person looking for a general synopsis of the current trends in education computer technology. It does, however, provide contacts for the researcher interested in a related area and therefore the book should appropriately find its place in many educational institutions.

It becomes evident on reading the book that limited resources and very substantial structural impediments are making the movement of many schools into the Information Age very difficult. Fortunately there are bodies of schools even in unlikely places, that have made a significant change and it is strongly suggested that the way forward is to assemble an infrastructure that will enable schools to continue to make meaningful contributions.

Largely the world around us is changing dramatically and the educational needs of students are facilitated through a model that has not changed fundamentally for the last century. The World Computer Conference and corresponding book represent an attempt to analyse current trends and prepare leaders to seriously vary underlying structures.

Despite immense efforts across the world by some visionaries, fundamental operations of departments and schools has not changed. The reality indicated by the book is that schools and other Educational Institutions around the globe are Industrial Age Organizations developing a very good Industrial Age product. Unfortunately their relevancy in a contemporary world is being questioned and many of the papers reflect the need for education to adjust to the computer and communication revolution.

Learning in schools is largely paper based, with Information Technology having made little impact on the majority of classrooms. Although the World Computer Conference facilitates some creative thinking and certainly the book displays a wealth of expertise, largely a small proportion of teachers possess the expertise and confidence to use IT extensively in their teaching.

The challenge ahead for most major Educational Institutions is considerable. The book indicates that a handful of people and schools are making significant inroads and changes to their operations and increasingly providing an education that is more in keeping with the needs of the information age and beyond. For the time being the question remains — will technology change the way education is conceived and delivered? Only time will tell.

The "World Conference on Computers in Education VI WCCE '95 Liberating the Learner" makes a significant contribution to the theme — "Liberating the Learner". Its subject content will be of some importance to those concerned with computers and education and may assist in some areas to generate enthusiasm and creativity. To accommodate such a broad range of topics the book is over 1,000 pages in length. Although the book provides contact names and email addresses, it could be of immense benefit to see a greater interaction and connectivity via the Internet. For example much of the material could be posted on the Internet allowing for the wider educational community to access and contribute to the information provided. Usenet Newsgroups would further add to the communicative process and provide feedback or generate healthy debate. As long as the recommended retail price is reasonable this is one book that should be included on the shelf of any Educational Institution that has an interest in Information Technology,

Michael Waldeck
Calvary Christian College


This volume contains part of the proceedings of the Second International conference on Curves and Surfaces which took place in Chamonix, France in June 1993. A total of 106 papers were presented at the conference, of which 58 are printed in this volume with the other 48 being published in the volume on Wavelets, Images and Surface Fitting.

The survey and research papers presented in this volume cover aspects on curves and surfaces, particularly as they relate to computer-aided geometric design. The topics covered include:

- Rational and constrained approximation, e.g. rational Bezier curves, Padé approximations, NURBS
- Spline conversion techniques and knot removal strategies
- Surface intersections, corner cutting and clipping
- Uses of object oriented programming
- Finding shortest paths on surfaces

The papers will be of use to researchers in the area and also for those implementing these techniques for particular applications. Unfortunately, for those wanting to keep at the forefront of the field, the articles are a little dated, as they were originally presented in 1993.

Jagoda Crawford
Australian Nuclear Science and Technology Organisation


These books are English translations of the Russian versions which were published in 1989. The first by Bakushinsky and Goncharsky is a theoretical treatment of ill-posed problems and has minimal interest for computer people.

The second, which was published before Tikhonov's death, is a theoretical treatment of linear ill-posed problems with or without a priori constraints. It does not cover the iterative regularisation algorithms although iterative methods are described for the construction of regularising algorithms.

It is written for those who wish to understand the theory behind the subject and it goes into some detail concerning practical problems. Approximately 70 pages of Appendix are devoted to Fortran listings of programs for the solutions of various types of Fredholm integral equations. In addition many subroutines are included in the earlier chapters. However, it would be extremely tedious for anyone to input all these Fortran code to a computer and the rather high price might be more justifiable if a floppy disk containing the Fortran code had been included.

This is a very rapidly developing subject, which is dominated by the Russians, and the translators have added a Postscript, of less than four pages, in an attempt to bring it up to date. The references in this Postscript are not included in the otherwise extensive Bibliography which does include 220 references.

In summary, these books are relatively expensive and for the numerical analyst who can afford only one, the second by Tikhonov et al is better value for money.

Godfrey N Lance
ANU and Bermagui, NSW

Jan L Harrington's book is marketed to aspiring Macintosh C++ programmers as 'your fastest way to learn object-oriented programming with C++ from the ground up.' It is a glossy package consisting of a thick paperback book and a CD-ROM containing a C++ development environment, the commercial CodeWarrior product from MetroWerks. The reader can install and run the development environment on their own suitably-equipped Macintosh. Despite the claims on the book's cover, the version of CodeWarrior on the CD is of very little use for any purpose other than compiling and running the sample programs also provided on the CD. It is essentially a demonstration version, labeled on the CD as CodeWarrior Lite.

The book's preface suggests two ways to use the book: as an introduction to programming for a non-programmer, or as an introduction to C++ for a programmer unfamiliar with C++. Reading guides are provided for these two options. Suggestions are oriented to individual readers rather than classroom use. Readers are expected to be knowledgeable users of the Macintosh operating system.

The book initially introduces fundamentals such as machine code, higher-level languages and automated translation, along with encoding schemes such as binary, ASCII, and so forth. This is followed by a very brief overview of object-oriented programming. Chapter 3, 'Using CodeWarrior', introduces the development environment with a simple C++ program. This chapter shows how to use the editor, create a C++ program including multiple source files, compile and run the program, deal with errors, and use the debugger. Chapters 4 through 11 each concentrate on a different language feature, including classes, input/output, arithmetic, strings, and pointers. Most chapters present at least one sample program which is provided on the CD. Many chapters include one or more 'Programming Challenges', exercises in modifying sample programs. Chapter 12 is titled 'Pulling it Together: The Checkbook Program', and it presents a simple cheque account manager program. Chapters 13 through 16 return to covering particular language features: operator overloading, data structures, and inheritance. The final chapter introduces the direct use of Macintosh operating system features to implement programs with a proper user interface. (Until this point the book employs the standard C++ input/output libraries, which at run time create a traditional terminal-like interface on the Macintosh screen.) There is no bibliography, apart from the final chapter's list of three books on Macintosh OS programming. An index and glossary are provided.

This book teaches the reader a little about CodeWarrior, something about C++, and touches upon programming for the Macintosh OS. As a self-study tutorial, the book is attractive for its simple structure and its use of listings, diagrams, and screen reproductions. It should be possible for a non-programmer, using this book, to quickly learn how to use CodeWarrior and write small C++ programs. After that, the book provides little direction. It is not really usable as a reference, yet it provides no pointers to any, not even to Stroustrup (1991). I expect that a programmer using this book to learn C++ would soon grow frustrated, since the software provided does not support much more than minor modifications to the sample programs. Academics would find the lack of rigour in descriptions of language features disappointing.


The evolution of systems development methodologies (SDM) shows how some have expanded their scope as an appreciation of the areas critical to the successful development of information systems has changed. For example, Jackson Systems Programming became Jackson Systems Development. In the same way, people are now looking beyond SDMs to project management techniques, to discover means by which existing SDMs can be integrated into accepted project management practices.

Structured Systems Analysis and Design Methodology (SSADM) is one of the better known methodologies and is primarily used in the development of large systems. SSADM has its home within the British Government Centre for Information Systems (COTA). PRINCE is the project management method recommended by CCTA to government departments for computer projects. It is, therefore, hardly surprising that this book, which provides a detailed description of work with these two methods, has been written.

Colin Bentley has over twenty years experience in the information technology industry, and was one of the original JSP lecturers. He has first hand experience of SSADM and PRINCE. Bernadette Rudman is a senior SSADM consultant. Their impeccable credentials are reflected in the quality of this book.

The book begins with an overview of SSADM and of PRINCE and then proceeds to a detailed description of the SSADM stages indicating how they dovetail with PRINCE. Also included are descriptions of the tools and techniques used within SSADM. Their description of SSADM has been assessed to conform with SSADM version 4 by the Technical Committee of the International SSADM Users Group.

The popularity of SSADM has ensured that there are many books which cover this topic. Many of these books, however, have not caught up with version 4 of SSADM, nor do they go into it with the depth that this book achieves. The descriptions of the steps and tasks are precise and lucid as would be expected from people involved in training practitioners in SSADM.

I think the real value of this book is its presentation of an SDM in the context of its relationship with project management. SSADM provides no guidelines on the organisational aspects of a project, so PRINCE is used to fill that gap. There is discussion of the variations in terminology between the two systems, and where structures overlap, and where there is a convergence of function, such as their examination of the quality review process.

This is a book which will be of benefit to practitioners as well as academics interested in the development of SDMs. My one criticism is that more time should have been given to the description of PRINCE. I imagine that information on PRINCE is relatively easy to come by in the UK, however, that is not the case here. Including such information would make the book much more valuable outside the UK.

John Lamp
University of Tasmania


This book achieves the authors' objectives in clear, concise language. The book is aimed at the networking professional, giving plenty of practical information and advice drawn from the authors own experience. I found the treatment of each topic sufficient to get a good grasp of the basics, while detailed enough to get real work done without wading through pages of tables and charts.

Starting with fundamentals of various network types, network operating systems, and network protocols, the text quickly settles down to a description of network protocols. Along the way, the authors share snippets of advice clearly drawn from real situations. Every section includes a number of simple figures which illustrate the fundamental elements presented in the text. The figures are refreshingly consistent in style throughout the book, providing a simple mechanism for comparing the features and design of the various operating systems, protocols and network topologies.

As a practical guide for network managers, the book emphasises practical problems and solutions in a logical, straightforward manner. As a basic reference or introductory handbook for professionals new to the day-to-day realities of network management, I would recommend this book highly. For those looking for detailed reference material, this book will disappoint. However, you might like to look out for the second and third books in the series if you are in need of a clear guide to NetWare or Microsoft's BackOffice.


This book is a collection of fifteen chapters covering a wide spectrum of areas. Organised around the title categories, the 'Systems' section contains chapters grouped under the headings Technology, Interfaces, and Techniques. Within the 'Applications' section are chapters grouped under Simulation, Education, Publishing, and Futures. There is a heavy UK bias to the book, with only two
of the fifteen chapters having first authorship from outside the UK; those two exceptions are from the US.

The quality of the chapters varies. Some seem perfunctory collections of "what we are doing". On the other hand, the majority of chapters contain thoughtful and thorough coverage of particular issues within their scope of interest. The best chapters either lay out particular challenges and then address how they have developed systems that pose solutions, or present a list of guidelines that cover a particular area. In the former category, the chapters on intelligent interfaces, the pragmatics of industrial use, hypermedia information management, animated diagrams, multimedia in education, and visual help all present interesting and valuable results. In the latter category, the chapters on essential elements, evaluation, and copyright issues are very worthwhile.

The book includes a CD-ROM, which has the text of the book and diagrams available, as well as audio and video clips to enhance the discussion. While the text of the book does not reference the CD-ROM elements, the online version is hyperlinked to those elements, and has an interface to support navigation. However, the CD-ROM only works on Windows machines, ignoring the Unix and Macintosh markets (although several chapters clearly present implementations on those platforms).

The book is an interesting compendium, but it is hard to identify the target audience. It covers a wide variety of topics and presents a considerable number of interesting ideas. On the other hand, it doesn't serve as a definitive introduction to the field, with rather idiosyncratic coverage of areas. Instead, it provides an eclectic survey of the field, but one that will only make sense to people already engaged in multimedia. However, the chapters are generally well written and as mentioned before, contain some new thoughts. I would recommend it as a supplementary reading for those who have been introduced to the concept of multimedia and are interested in seeing a variety of issues and ways in which it can be used.

Clark Quinn
Open Net Pty Ltd


This book is a detailed guide about how to build information systems based on the Internet. The challenge for managers, developers and users is to integrate such electronic sharing systems into existing corporate information structures. The author discusses issues that arise from gathering and disseminating information (both internally and externally) using Internet technology. AT&T, Lockheed Martin and IBM are examples of companies that have already constructed comprehensive internal webs of enterprise information.

The popularity of the Internet has fuelled a demand for a wider sharing of corporate information than ever before, both internally (status reports, project documentation, departmental publishing, memo archives, etc.) and externally (product catalogues, customer support services, direct sales, press releases, etc.).

To collaborate successfully on today's complex projects, workers need more than just access to the company library and local colleagues. The coupling of Internet technology (in particular the World Wide Web) with enterprise information provides business opportunities that were previously unavailable.

This book has not been written to describe the inner workings of the Internet in detail. Rather it is, as the author describes in his own words, "about an approach to information handling and sharing that is characteristic of the Internet".

The first few chapters of the book provide an overview of what the Internet is (and isn't). The concept of corporate Internet clones is introduced, followed by discussion about the current state of Internet technologies and tools — Simple Mail Transfer Protocol (SMTP), Electronic Data Interchange (EDI), Bulletin Boards, File Transfer Protocol (FTP), Wide Area Information Server (WAIS), Gopher, plus other miscellaneous Internet tools. A separate chapter is devoted to the World Wide Web (WWW).

The remainder of the book looks at the practicalities of building Internet clones. Topics covered include dealing with legacy data, security, evaluation of alternative solutions, specification and implementation of a clone, and issues involved in operating and maintaining a system once it goes into production. Another chapter looks at planning for the future, and discusses both cultural and information technology trends.

The final chapter asks if building an Internet clone is worth it. (A purely rhetorical question given the existence of the book!). Sprinkled throughout the book are email addresses and URLs (Uniform Resource Locators). These can be followed up for more information, for example, papers that have been delivered at WWW conferences, product information, and so on. The book concludes with a list of references and two appendices.

The first appendix discusses the concept of the client/server model. It has been included since the Internet is regarded by many as the biggest accumulation of client/server systems. The second appendix outlines the steps involved in undertaking an Internet pilot project (a pilot program is recommended before tackling the construction of a mission critical, enterprise wide Internet-based information system).

Tony Stevenson
Melbourne


This book is advertised on the back cover as supporting the reader to "learn how to create high-quality multimedia designs". And, with some constraints, it will support this. However, these constraints require caution on the part of potential purchasers.

The book breaks down multimedia graphic tasks into several categories. After an introductory chapter, the graphic tasks are broken down into backgrounds, buttons and controls, text, interactive techniques, presentations, and the World Wide Web. Each chapter covers some standard graphic techniques that are relevant to the category. The text is copiously illustrated and annotated.

The major constraint is that this book does not provide a conceptual overview. Such an overview is essential if the reader is going to be able to generalise from the specific examples provided, to other tasks. Essentially all of the techniques used are given as procedures without providing an underlying model. For example, in producing a background from a bitmap, the reader is instructed to use the "auto-trace" function to produce polygons, without any explanation of the relationship between the two. While it is not a difficult inference, the presentation does not address the options that are available within auto-trace, and how they would affect the results. The book also has an idiosyncratic approach to terminology; most of the terms are introduced but a few specialist terms are used without introduction. For example, I don't know why 'fat-bits' should be any more familiar than, say, 'pixels', but only the latter is defined.

As a more minor quibble, there are some omissions in the presentation. For instance, the common distinction between 'radio buttons' and 'check boxes' is that the former are for mutually exclusive options, while the latter has no such constraints. This fundamental difference is submerged in the description. Later on, it is implied that the scripting will work for both HyperCard and SuperCard, but the code examples require capabilities that only SuperCard provides.

The book also uses particular packages to illustrate the techniques. SuperPaint and SuperCard figure prominently. It seems likely that the approach will generalise to other packages in many instances, but some work may be required and there is no guidance for a general approach to this. This could be a weakness for some readers.

That said, this book could serve admirably as a reference work. It has many techniques I've wanted to know how to do, such as bevelled buttons, etched text, and more, all clearly explained. The book describes the process and shows an example, typically with a close-up so you can see the fine detail. Similarly, detailed scripting examples illustrate the interactive techniques. The book is only shades of grey, but includes a CD-ROM with not only all the graphics in colour, but also a large collection of utilities and information to support the described tasks. If you're not a graphic person but have a need to make good looking presentations, this book will show you how to produce the professional looking components. This is not a text on graphic design, as the text notes, you are still responsible for arranging the components into an overall design, but as a resource for the independent designer this book is a storehouse of techniques. If you want to know how to do the things this book covers, this book will show you how.
Computer telephony (CT) is the synthesis of computers and telephones to deliver superior business solutions to those that are currently derived from computer or telephone technology used in isolation.

By combining computers and telephones, highly functional systems can be built which incorporate call logging, computer-based faxing, voice mail, and autodialing. Used in conjunction with personal information managers (as well as other sorts of customer databases), calendar and scheduling software, electronic telephone and address books, new levels of efficiency can be attained in the modern office.

For example, in a help desk environment, an operator can be equipped with a CT system which recognizes callers before the operator picks up the ringing telephone. Using Automatic Number Identification (ANI), which is the technology on which caller identification is based, the caller is recognised between the first and second rings. So in the time that it takes the call to be answered, the system has already issued a database search which returns a list of calls previously made by the person now requesting more help.

This book is aimed at small office and home office (SOHO) users of CT. But, because many developments in telephony originally occurred in larger systems, references to these higher end systems are also included throughout the book.

The authors’ goals are:
1. to provide knowledge of the technology, functionality, and costs associated with this relatively new field of information processing;
2. to describe the CT hardware and software which is currently available;
3. to provide the knowledge to either personally install a CT system or to hire (and then work with) a consultant;
4. to include further references which readers can turn to for the latest information relating to CT.

The book has been divided into three parts and three appendices.

Part one, a technical overview, defines CT and what is required to make it work. Topics covered include analog and digital communications, services and functions, how to network the telephone, and the technical specifications underlying telephony.

Part two looks at the technology available such as caller ID, speech and voice recognition, call logging, inbound call screening, smart agents, etc. One chapter can be used as the basis for determining an individual’s or organisation’s telephony needs, whilst another chapter concentrates on CT interfaces.

Part three explains how to get started with CT. It provides information about choosing the most suitable hardware and software, the steps required in preparing for and then installing a SOHO system, as well as sections on testing/troubleshooting, and answers to FAQs (Frequently Asked Questions).

The first appendix is a comprehensive CT bibliography and reference to online resources. Appendix B contains vendor information (geared towards the American market) while the last appendix is a useful glossary of CT terms and acronyms.

This book is aimed at small office and home office (SOHO) users of CT. But, because many developments in telephony originally occurred in larger systems, references to these higher end systems are also included throughout the book.

The authors’ goals are:
1. to provide knowledge of the technology, functionality, and costs associated with this relatively new field of information processing;
2. to describe the CT hardware and software which is currently available;
3. to provide the knowledge to either personally install a CT system or to hire (and then work with) a consultant;
4. to include further references which readers can turn to for the latest information relating to CT.

The book has been divided into three parts and three appendices.

Part one, a technical overview, defines CT and what is required to make it work. Topics covered include analog and digital communications, services and functions, how to network the telephone, and the technical specifications underlying telephony.

Part two looks at the technology available such as caller ID, speech and voice recognition, call logging, inbound call screening, smart agents, etc. One chapter can be used as the basis for determining an individual’s or organisation’s telephony needs, whilst another chapter concentrates on CT interfaces.

Part three explains how to get started with CT. It provides information about choosing the most suitable hardware and software, the steps required in preparing for and then installing a SOHO system, as well as sections on testing/troubleshooting, and answers to FAQs (Frequently Asked Questions).

The first appendix is a comprehensive CT bibliography and reference to online resources. Appendix B contains vendor information (geared towards the American market) while the last appendix is a useful glossary of CT terms and acronyms.

The book has been divided into three parts and three appendices.

Part one, a technical overview, defines CT and what is required to make it work. Topics covered include analog and digital communications, services and functions, how to network the telephone, and the technical specifications underlying telephony.

Part two looks at the technology available such as caller ID, speech and voice recognition, call logging, inbound call screening, smart agents, etc. One chapter can be used as the basis for determining an individual’s or organisation’s telephony needs, whilst another chapter concentrates on CT interfaces.

Part three explains how to get started with CT. It provides information about choosing the most suitable hardware and software, the steps required in preparing for and then installing a SOHO system, as well as sections on testing/troubleshooting, and answers to FAQs (Frequently Asked Questions).

The first appendix is a comprehensive CT bibliography and reference to online resources. Appendix B contains vendor information (geared towards the American market) while the last appendix is a useful glossary of CT terms and acronyms.

The book has been divided into three parts and three appendices.

Part one, a technical overview, defines CT and what is required to make it work. Topics covered include analog and digital communications, services and functions, how to network the telephone, and the technical specifications underlying telephony.

Part two looks at the technology available such as caller ID, speech and voice recognition, call logging, inbound call screening, smart agents, etc. One chapter can be used as the basis for determining an individual’s or organisation’s telephony needs, whilst another chapter concentrates on CT interfaces.

Part three explains how to get started with CT. It provides information about choosing the most suitable hardware and software, the steps required in preparing for and then installing a SOHO system, as well as sections on testing/troubleshooting, and answers to FAQs (Frequently Asked Questions).

Ahuja provides concise material, and liberal references to other sources for those seeking more detailed information. This is not a lightweight treatment of the subject, however, as the author takes care to provide some theory along with plenty of examples of real problems and practical solutions. After a brief run through some historical background, the author moves on to cover logon and authorisation issues. This provides background for the discussion of securing workstations, distributed security services and access control. The final three chapters cover Internet security, firewalls and security management.

Having dragged this book around with me for a while now, I find it is certainly covering the subjects aimed for. I have found the book handy for hints as to what, where and when to look for more information about network security. This book is probably more for those who are beginning to become more involved in network security, or are looking to set up a network for the first time and need a place to start.

Tony Stevenson
MKD Software Consulting


The author targets the book at the professional with a need or desire to understand and enhance network security, and gives a good foundation for further, more specific reading.

Ahuja provides concise material, and liberal references to other sources for those seeking more detailed information. This is not a lightweight treatment of the subject, however, as the author takes care to provide some theory along with plenty of examples of real problems and practical solutions. After a brief run through some historical background, the author moves on to cover logon and authorisation issues. This provides background for the discussion of securing workstations, distributed security services and access control. The final three chapters cover Internet security, firewalls and security management.

Having dragged this book around with me for a while now, I find it is certainly covering the subjects aimed for. I have found the book handy for hints as to what, where and when to look for more information about network security. This book is probably more for those who are beginning to become more involved in network security, or are looking to set up a network for the first time and need a place to start.

Steven Clark
Northern Territory University


For some years, formal specification techniques have promised much but delivered little. This book is a revision of the author’s doctoral thesis in the research area of formal specification techniques. It presents the specification language LCL, together with a non-trivial example of the practical application of formal specifications. It also presents a way to use redundancy in specifications, and a style of using abstract types in Standard C.

Larch is a family of specification languages, the first of which was completed in 1980. Each member of the family is a two-tiered language such as Larch/Ada, Larch/Smalltalk, or the Larch/C Interface Language (LCL) presented in this book.
After an introduction, Chapter 2 presents a brief overview of LCL, showing how it can be used to specify functions and abstract types. Chapter 3 shows how LCL specifications can support data abstraction and modularity in C programs. There is a description of the tool called LCLint, which checks LCL specifications against C programs. Chapter 4 introduces the PM program, the subject of the case study that makes up the next few chapters. This chapter also presents some techniques for writing specifications by walking through some of the specifications of the PM program. Chapter 5 introduces the idea of claims — redundant information in a specification in the form of assertions. The chapter shows how claims can support program testing, help detect errors in specifications, and help to document specifications. Examples illustrate the use of claims for these purposes. Chapter 6 discusses the application of LCL specifications to the re-engineering of the PM program. A re-engineering process model is presented, with an account of how it was applied. The effects are presented. Finally, the software tools employed are listed — specification syntax and type checkers, proof checker, specification translator, specification library, and the consistency checker LCLint. Chapter 7 provides a restricted formal overview of LCL, including the language’s basic concepts, storage and types, and semantics for functions and modules. Chapter 8 summarises the research and suggests further research directions.

Appendices A through E present a considerable amount of supplementary information: a reference grammar for LCL, supplementary information about LCL types and operators, references to electronic sources of Larch tools and documentation, and a complete listing of the specifications for the interfaces considered in the case study. A bibliography and index are provided.

Despite this book’s academic origins I think it could be of some use to those constructing or maintaining standard C modules. It comes with an important recommendation in the form of a foreword from John Guttag. It presents a way of introducing formal specification without requiring programmers to abandon standard C. Formal specification is a topic that is difficult to present to non-academics, but for a book based on a dissertation this one manages to avoid undue opacity. The worst feature of this book would appear to be the cost. It is a valuable book, and people should read it, but I could not describe it as value for money at the price quoted for this review. If you can get it for less, do so.

DA Vincent

Hydrographic Sciences Australia


This book is a collection of papers which are based on those presented in the “Program Development Tools and Environments for Parallel and Distributed Systems” minitrack of the 28th Hawaii International Conference on System Sciences. The papers of this collection are grouped into four parts: mainstream program development tools; performance prediction tools and studies; debugging tools and research; and nontraditional tools.

In the first part, Ng et al introduce the Software Architect’s Assistant which is a visual programming environment for the design and development of distributed programs. It provides the user with automated, intelligent assistance through the software design process. Facilities provided include the display of integrated graphical and textual views, a flexible mechanism for recording design information, the automatic generation of program code, and formatted reports from design diagrams. The paper by Clemenccon et al presents ANNAI which is an integrated environment consisting of an extended High Performance Fortran (HPF) compiler, a performance monitor and analyser, and a source-level debugger for distributed programs, all sharing a common user interface. Users can mix data parallel programming with a message passing paradigm.

The paper by Cheatham et al describes H-BSP which is an environment for developing transportable algorithms. Based on that model, a program’s performance can be expressed as a function of a few architecture independent parameters. Therefore, a BSP-L compiler should be able to choose one of several codes to implement the same function based on the parameters describing the architecture it is ported on. Feldcamp and Wagner introduces the Parsec parallel programming environment with emphasis on its performance aspects. Parsec comprises a resource allocation and mapping tool and a load configuration tool with a visual user interface. It is intended to support the development of message passing programs.

In the second part, the N-MAP tool by Ferscha et al is dedicated for early performance prediction. From a skeletal representation of a parallel SPMD program, N-MAP automatically generates a discrete event simulation program, the execution of which reflects the behaviour of the skeletal parallel program. Hansen introduces PATOP, an interactive performance analysis tool, that can analyse program performance on massively parallel computing systems. A major feature contributing to the scalable representation of program data is the ability to focus measurements on points of interest in the program execution by specifying behavioural attributes. Behavioural attributes are given as thresholds to the results of other measurements. Kotsis et al’s paper performs a study evaluating five of the most commonly used tools (namely PVM 2.x, PVM 3.x, p4, Express and Linda) with respect to efficiency and also ease-of-use using four of the NAS benchmarks.

In the third part, Hood and Cheng’s paper pushes for a client-server approach in building a debugger for distributed computations that run on a heterogeneous set of machines. Such debuggers are commonly built by layering a sophisticated user interface on top of existing sequential debuggers. In that approach, the client user interface can be paired with a variety of server implementations via a precise interaction protocol. The paper by Garg et al discusses efficient detection of global predicates in a distributed program. They introduce the concept of a channel predicate and provide an efficient algorithm to detect any boolean formula of local and channel predicates.

The fourth part deals with approaches which radically differ from a majority of the efforts in tool and environment building. Attali et al present a formal definition of the dynamic semantics of Sisal 2.0 which is an applicative language used in parallel programming. The authors built a visual environment for its execution which also allows the user to visualise the process of applying different semantics rules to his/her program. The paper by Collins and Brown discusses MATRIX++, a high-performance matrix computation environment. The specific problem it addresses is extending MATRIX++ to provide language and compiler support for matrix computations on distributed memory architectures. Wolff introduces a language-independent transparent approach for object distribution and remote inheritance. This approach provides mechanisms to support the needs of a designer of an object-oriented distributed program making it easier to concentrate on the application rather than its object-oriented implementation details.

In summary, this book is a reference for researchers and practitioners. Some materials can also be used for graduate level courses in software engineering and parallel and distributed systems.

Daniel KC Li

Macquarie University
NEWS BRIEFS

"News Briefs" is a regular feature which covers local and overseas developments in the computer industry including new products and other topical events of interest.

IT INDUSTRY LIABLE FOR 'YEAR 2000' PROBLEMS

Software developers, vendors and maintainers should all urgently check their liability insurance.

Virtually any organisation operating in the software sector is highly exposed to legal action as a result of the 'Year 2000' problem. (The Year 2000 problem is caused by computer software that is unable to perform using dates with '00' as the year).

While most organisations know about the problem, few in Australia have done anything about it. "This lack of action could result in substantial costs for them in the new millennium", warns Mr Mark Feetham, technology partner at leading commercial law firm Middleton Moore & Bevins.

He says: "There are very significant liabilities for software companies if their clients experience Year 2000 problems and goods or services supplied by those clients are faulty or defective as a result".

"If, for example, the software used in transport or medical applications fails due to a Year 2000 problem, the supplier of the software would potentially be liable for any death or injury to persons which occurred".

Mr Feetham says this liability extends to virtually all organisations in the software supply and support industries.

"Licensors who have supplied software susceptible to the Year 2000 problem or consultants who have recently recommended the purchase of such software are similarly potentially liable".

"Software maintainers are also potentially liable to resolve any Year 2000 problems in software they were under contract to maintain".

"Damages could be sought from all these groups of suppliers under Section 52 of the Trade Practices Act if they engaged in misleading or deceptive conduct in relation to the Year 2000 problem. A typical situation would be where a licensor had represented as not susceptible software that later turned out to be exposed to the Year 2000 problem".

"As for those software maintenance contracts which were executed after the Year 2000 problem became widely known, say this year, they potentially require the maintainer to bear the cost of rectifying any Year 2000 defect in the software which they maintain".

"Vendors or consultants supplying software should be careful to inform customers likely to use the software after 2000 whether or not it is Year 2000 compliant".

Mr Feetham also warned businesses looking at new contracts for software supply or support to be aware of the problem and the responsibilities of the supplier and maintainer.

"All maintenance agreements which are entered into from now should expressly deal with the Year 2000 problem. If a proposed supplier will not amend a standard agreement to specifically include it, the best advice is to find another supplier".

FINDIT! FAST! FOR FREE!

An interactive Australian business directory called Cowleys FindIt! is helping small businesses to promote themselves and their products on the Internet.

Aimed at small to medium businesses, the directory already lists over 830,000 Australian businesses free of charge.

The directory is used by people who are finding the Internet is an efficient way to locate Australian products and services, without having to look through telephone books, business directories, restaurant/accommodation guides etc.

"FindIt! is an easy way for new businesses to be on the Internet", says Scott Williams, Managing Director of Cowleys FindIt!. "You don't need a Web address to be in the directory".

Where a Web address is known, it is automatically merged into the listing. The same goes for E-mail. Over 7,000 businesses which already have a Web site automatically have their directory listing hot linked to their site.

Special interest groups within FindIt! allow rapid searching. For example, legal and business services, consultants, dining, accommodation and agricultural products and services can all be located quickly.


INTERNET INTEREST NETS MAJOR MALAYSIAN DEAL

Macfarlane Generators has joined the information 'super highway' ... with immediate results.

Within days of going on the Internet, Australia's generator specialists picked up a major export order from Malaysia ... significantly the company's largest single order ever outside a government contract.

A Malaysian forestry firm had accessed product and price details from Macfarlane's Internet page, and promptly arranged a visit here to check stock first-hand.

An order quickly followed for three 850 kVA Dorman generator sets, all pre-owned with low hours, and fully serviced and detailed at Macfarlane's Melbourne headquarters.

Macfarlane Generators' Internet-led order is the first of its kind for the company, and demonstrates the potential business that could result from such an accessible worldwide communications system, according to Managing Director Gerald Kay.

"Within days of initially putting our brochure and prices on the Internet we were receiving enquiries, and that has grown steadily in the months since then", Gerald Kay explains.

"We have always done quite a bit of business overseas, but the Internet has certainly increased interest and speeded up the whole process. It took just six weeks to deliver the Dornans to Malaysia from the time the enquiry was first received".

Macfarlane Generators' information page on the Internet features an overview of the company's products and services, and up-to-date pricing. It can be accessed on: http://www.ozemail.com.au/~macgen

THE PARLIAMENT OF NEW SOUTH WALES ON THE INTERNET


The Parliament of New South Wales' Internet Site was launched on 29 October, 1996, at Parliament House, Sydney, by the Hon. Max Willis, MLC, President of the Legislative Council and the Hon. John Murray, MP, Speaker of the Legislative Assembly.

Speaking at the launch, Mr Willis said: "The development of this site gives the people of NSW unprecedented information about the workings of democracy in this State. It will provide quick and easy access to the most comprehensive and up-to-date bank of information about the Parliament, its Members, operations and activities".

Mr Murray said that the site would be particularly useful for local researchers, students and the media but could be accessed from anywhere in the world. "This will be a valuable education and business resource and is part of the Parliament's ongoing commitment to openness and accountable government".

"The information stored on the site will be kept up-to-date, and where appropriate will be amended every day".

"Parliament is committed to best practice in information provision and views this site as only the beginning of the use of this form of accessible technology. The site will be constantly under review and development, and feedback and ideas for improvement will be welcomed".

Most Departments and Sections of the Parliament were involved in the development of the site under the direction of the Parliamentary Education and Community Relations.

For more information contact Parliamentary Education and Community Relations Manager, Helen Williams, on 9230 2334.


A CHARACTER-BUILDING PROJECT

To be literate in Japanese, it is necessary to learn some 2,000 Kanji characters.

For the 180,000 Australians studying Japanese at High School, TAFE and University, additional help is now available with a sophisticated extension of the Kantaro computer software package. Kantaro, Volume 1, was first launched three years ago as a joint project between Fujitsu Australia Limited and Macquarie University. The new advances are expected to revolutionise Japanese teaching.

The initial package, which covers 200 basic Kanji (including all the characters required for the New South Wales Higher School Certificate), was developed by Macquarie University's Japanese department and Fujitsu Australia, and was an instant international success.

Trialled by first-year language students at Macquarie University, the multimedia package was then endorsed by the New South Wales Board of Studies and rapidly adopted by many businesses and educational institutions throughout Australia.
Australian and New Zealand universities, TAFE colleges and secondary schools. Several leading universities in Japan now use it to teach Japanese to foreign students and last year Kantaro was introduced in the USA.

Volume 2 and 3 of Kantaro add another 500 Kanji and target different areas of learning difficulties. They're aimed at intermediate-standard Japanese students and build on the original user-friendly animated graphics and CD-ROM sound in the Windows-based program.

Students can learn at their own pace and benefit from non-traditional learning techniques such as the extensive use of mnemonics (memory aids). Students see, for instance, the picture of a tree gradually changing to the Kanji symbol for a tree, using morphing techniques. Dynamic animation also shows the stroke order to write each Kanji, games reinforce learning and, in the final module, original reading materials are linked with a dictionary-type database to avoid student frustration with unfamiliar Kanji. One click of the mouse brings up the necessary information instantaneously, avoiding the tiresome process of referring to a number of dictionaries. This advance will be one of the major selling points for the new packages.

**DESTINATION QUEENSLAND!**

The Queensland Tourist and Travel Corporation (QTTC) has launched the newest way to access Queensland's vast array of tourist attractions and facilities — its Destination Queensland Internet site.

Destination Queensland provides consumers and the travel industry with more than 1,800 pages of destination and product information and images, travel tips and general information on Australia's Sunshine State.

It was launched by journalists using the site for the first ever Cybertour of Queensland.

The Chief Executive Officer of the QTTC, Stephen Gregg, said Destination Queensland was the most comprehensive site of its type in Australia.

"It contains a database of more than 2,400 Queensland tourism products from 750 operators, as well as information on destinations, attractions, events and Australian travel tips", he said.

"Destination Queensland will be an invaluable resource for inbound tour operators, travel agents, wholesalers and consumers, and an important distribution mechanism for tourist operators"

"It will be particularly useful to small and niche operators who would otherwise find the international market difficult to penetrate".

"Its ease of navigation makes Destination Queensland accessible to everyone from Internet amateurs to seasoned Net surfers"

The QTTC utilised the expertise of its Sunlover Holiday reservations staff, who are experienced in using electronic booking systems, to ensure the system is user-friendly. Mr Gregg said that under an agreement brokered by the QTTC and the Inbound Tourism Organisation of Australia, international visitor bookings would be made directly on the system through inbound tour operators in 1997.

Domestic travel agents will be able to access the information and eventually use a real-time booking system. Consumers can use electronic mail to request more information about products featured on the site.

The Web site was developed by the QTTC with the assistance of Telstra Multimedia. It has been enthusiastically embraced by tourism operators.

The site will eventually contain an extensive range of QTTC information including tourism statistics, travel stories, media releases and publications.


**$11 MILLION GOLF CONTRACT**

Unisys Australia has entered into an $11 million agreement with the Australian Golf Union to introduce a high-tech national computerised handicapping system for amateur golf.

A world first, the innovative system — called 'GOLF Link' — will connect Australia's 1,600 golf clubs and their members through a central computer system.

The system will be based around a GOLF Link plastic swipe card and utilises EFTPOS type terminals, existing club facilities and a central computer system to manage the handicapping details of Australia's 500,000 men and women club golfers.

Every club golfer in Australia will have access to the GOLF Link system, which can be used to verify membership, confirm handicaps and enter competitions through the use of computer terminals.

Unisys will design and operate the network, write the software and implement the database system. The implementation of the GOLF Link system through 1,600 clubs is expected to take 18 months to complete and will commence with the installation of hardware early this year, with the first clubs coming on line from June 1997.

GOLF Link allows for instant handicap verification as a player's up-to-date handicap can be accessed at any time from any club in Australia by a player simply swiping his or her card through the terminal.

Under the agreement, Unisys has committed $3.1 million as a platinum sponsor of the Australian Golf Union to introduce a high-tech national computerised handicapping system for amateur golf.

A world first, the innovative system — called 'GOLF Link' — will connect Australia's 1,600 golf clubs and their members through a central computer system.

The system will be based around a GOLF Link plastic swipe card and utilises EFTPOS type terminals, existing club facilities and a central computer system to manage the handicapping details of Australia's 500,000 men and women club golfers.

Every club golfer in Australia will have access to the GOLF Link system, which can be used to verify membership, confirm handicaps and enter competitions through the use of computer terminals.

Unisys will design and operate the network, write the software and implement the database system. The implementation of the GOLF Link system through 1,600 clubs is expected to take 18 months to complete and will commence with the installation of hardware early this year, with the first clubs coming on line from June 1997.

GOLF Link allows for instant handicap verification as a player's up-to-date handicap can be accessed at any time from any club in Australia by a player simply swiping his or her card through the terminal.

Under the agreement, Unisys has committed $3.1 million as a platinum sponsor of the Australian Golf Union to introduce a high-tech national computerised handicapping system for amateur golf.

A world first, the innovative system — called 'GOLF Link' — will connect Australia's 1,600 golf clubs and their members through a central computer system.

The system will be based around a GOLF Link plastic swipe card and utilises EFTPOS type terminals, existing club facilities and a central computer system to manage the handicapping details of Australia's 500,000 men and women club golfers.

Every club golfer in Australia will have access to the GOLF Link system, which can be used to verify membership, confirm handicaps and enter competitions through the use of computer terminals.

Unisys will design and operate the network, write the software and implement the database system. The implementation of the GOLF Link system through 1,600 clubs is expected to take 18 months to complete and will commence with the installation of hardware early this year, with the first clubs coming on line from June 1997.

GOLF Link allows for instant handicap verification as a player's up-to-date handicap can be accessed at any time from any club in Australia by a player simply swiping his or her card through the terminal.

Under the agreement, Unisys has committed $3.1 million as a platinum sponsor of the Australian Open until 2001. As part of this platinum sponsorship package, Unisys will provide on-course scoring for the Australian Open, including media and leader-board score services. Already key sponsors of the US and British Open, the sponsorship deals strengthens Unisys' position in international golf.

GOLF Link offers significant benefits to players and clubs. For example, golfers will no longer need to provide handicap records when entering events.

Additionally, there will no longer be a need for clubs to return a visiting player's scorecard to his or her home club. The overall administration of the sport will be simplified by the system.

The move to the high-tech yet simple to operate handicapping system will be of particular benefit to the 800-odd clubs in Australia that currently use manual handicapping methods.

GOLF Link will allow the AGU to modify handicap and calculated Course Rating parameters at no cost to the clubs. It also provides the governing body with the capacity to gather statistical data that will assist in the development of the game.

**DICTIONARY OF INVESTMENT TERMS GOES ONLINE**

The Australian Financial Review Dictionary of Investment Terms from County NatWest has now been published in an on-line edition for users of the Internet.

The Dictionary, first published in 1989, was recently issued in its fourth edition by AFR Books in conjunction with County NatWest. It explains in clear and simple terms commonly-used words, expressions, abbreviations and acronyms, many of which are peculiar to the investment management industry.


Copies of the printed edition of the Dictionary can be purchased for $19.95 (plus $3 postage and handling) from Financial Review Books, PO Box N542 Grosvenor Place, Sydney NSW 2000; or by phone order on (02) 9238 7655 or 1800 251 949 (call-free outside Sydney area).

**ETHERJET PC CARD**

As organisations continue their move towards remote network computing, PC cards are becoming an essential peripheral device. Catering for this demand, IBM has launched a new EtherJet PC Card which forms part of the company's extensive Options product line.

EtherJet is the brand name of IBM's range of fully featured Ethernet adapters. These EtherJet adapters include full duplex capability, 'low DOS usage' and 'Wake Up on Lan' features. Mr Glen Foster, IBM's Product Manager - Options, said the Options range offers over 400 products designed to assist and improve network and standalone computing. Included are memory, storage products, networking adapters, and accessories for PCs, Thinkpads and PC servers.

"The EtherJet PC Card is a 10 Mbps adapter that provides special features for mobile users wishing to access network resources", Mr Foster said.

The card comes in two models, a 10BASE-T model and a combination 10BASE-T and 10BASE2 model, making it a viable option for users who require connection to both types of cabling.

A variety of operating and network operating systems are compatible with the EtherJet PC Card. They include Microsoft Windows NT (versions 3.51 and higher), Windows 95, Novell NetWare (versions 3.12 and 4.1) and Microsoft LAN Manager.

IBM manufactures a full range of Ethernet and Token Ring networking adapters for ISA, PCI and PCMCIA architectures.