Preface

> *Information is invisible, communicative, and laden with value and ethical implications* (Baird et al., 2000, p. 10).

Drawing on the earlier writings of Joseph Weizenbaum (1976), Stacey L. Edgar, in the introduction to his excellent book, *Morality and Machines*, emphasises the need to "examine the dangers of being too mesmerised by the 'computational theory of mind,' which can, with its deterministic and materialistic implications, lead to losing sight of what is of moral (and aesthetic) *value*" (2003, p. 7). Similarly, the renowned communications theorist Raymond Williams reminds us that "a technology is always, in a full sense, social. It is necessarily in complex and variable connection with other social relations and institutions … " (1981, p. 227). It is in a timely manner, therefore, that *Information Security and Ethics: Social and Organizational Issues* brings together a collection of recent work by international scholars addressing a number of significant and current social and moral issues associated with the development and use of new information and communication technologies.

The interrelated areas of information security and information ethics are rapidly gaining importance in the wake of the terrorist attacks on the USA on September 11, 2001 and at the same time as academics, computer professionals, government agencies, business organisations and the general public are becoming increasingly aware of the dangers associated with our growing reliance on computer technologies — particularly with regard to the ubiquitous and unregulated nature of the Internet. Today, all members of society are affected by computers - even if they themselves do not own one. The computer has changed our home and workplace environments, how we communicate, how we do business, how we shop and how our children are educated and entertained. As parents, we may be becoming more and more concerned about our inability to protect our children from what we perceive as the harmful effects of technology. As citizens, we may be growing increasingly anxious about the external threats to our national security posed by cyber-terrorists and the internal threat to us as individuals of government control and the related invasion of our rights to privacy and free speech. Business organisations, meanwhile, need to be constantly alert to the increasing dangers to their information security and intellectual property posed by hackers and white-collar criminals. The responsibility lies not just with managers. Kevin Day suggests that had all employees been educated in security then the majority of recent successful security attacks could have been avoided. "Security is not a technology; it is a thought process and a methodology" (Day, 2003, p. 4).

An uncritical acceptance of technological growth and development can and has provoked a series of ethical dilemmas. As James Moor warns us,

> *Computer sprawl, like urban sprawl, moves inexorably on many fronts unsupervised …[It] is worldwide and culturally transforming. Computer sprawl is not necessarily rational or harmless, but it is an undeniable force in the world that will affect not only the lives of all of us in technological societies but quite possibly everyone on the planet and their descendants for centuries to come. The ethics gap that is generated because we massively computerize without taking time to consider the ethical ramifications is therefore quite wide and deep* (Moor in Baird et al., 2000, pp. 35-36).

While the computer-literate amongst us may enthusiastically embrace new technological developments and the associated changes they bring to our lives, other groups such as the less educated, the aged, the disabled and those living in less developed nations are becoming increasingly marginalised and powerless. Just as C.P. Snow in 1959 alerted us to the dangers inherent in the gap between the members of the "two cultures" of the sciences and humanities within Western societies, a number of the authors in this volume attest that the world-wide gulf between the information-rich and the information poor - the "two cultures of the computer age" (Weizenbaum in Edgar, 2003, p. 2) - is rapidly widening. In order to achieve global ethical solutions to this major problem, "[members] of the scientific community must bring a greater technical understanding of the underpinnings of the technologies involved; those from the humanities must bring a basis on which to make moral judgements and choose social and political alternatives well" (Edgar, 2003, p. 3). As Edgar suggests, we would do well to consult the writings of founding moral philosophers such as Aristotle in order to establish an ethical framework adaptable to the Information Age.

At the same time, we need to be aware that, because of the rapid development of technology, it seems likely that there will always be an ethics gap between technology and its use (Baird et al., 2000). Nonetheless, it is through the ongoing, “cross-cultural” (that is, between the sciences and humanities as well as between local/regional cultures) and inter-disciplinary studies, debates and discussions undertaken by international scholars such as those present in this volume, that, hopefully, we may achieve greater global awareness and possible solutions to the ethical dilemmas we are now facing within technologised societies.

Organisation of the Book

The content of the book is organised into two parts: Part 1 (Chapters 1-8) focuses on Information Ethics; Part 2 (Chapters 9-14) focuses on Information Security. A brief description of each of the chapters follows:

Part I: Information Ethics

Chapter I: *MAMA on the Web: Ethical Considerations for Our Networked World* by Barbara A. Schuldt, Southeastern Louisiana University, USA, addresses the need to find a global solution to the ethical problems caused by the open nature of the Internet and the growth and diversity of its users. To this end, the author proposes the adoption of four categories to enable the definition and discussion of these ethical issues. This chapter provides a framework for the discussion provided by the authors of the following chapters.

Chapter II: *Establishing the Human Dimension of the Digital Divide* by Helen Partridge, Queensland University of Technology, Australia, considers the psychological factors contributing to the digital divide through an examination of Internet users and non-users in Brisbane, Australia and San Jose, California, USA. Through this study, the author aims to expand the understanding of this phenomenon in order to enable the development of strategies and programs to bridge the gap between the information rich and information poor.

Chapter III: *Socio-economic Influence on Information Technology: The Case of California* by Rasool Azari and James Pick, University of Redlands, USA, proposes the steps that need to be taken by the State of California in order to foster technology and reduce the digital divide. The authors emphasise the inter-relationship between socio-economic factors and technological development, warning that focusing solely on the equality of distribution of technologies is insufficient in solving the digital divide.

Chapter IV: *The Ethics of Web Design: Ensuring Access for Everyone* by Jack S. Cook, Rochester Institute of Technology, USA, and Laura Cook, State University of New York, USA, addresses the problem of Web accessibility for the disabled — including the aged and injured. The authors emphasise the need to educate Web designers — many of whom are unaware of the problem, as well as the need for laws enforcing Web access for all.

Chapter V: *Web Accessibility For Users with Disabilities: A Multi-faceted Ethical Analysis* by Alfreda Dudley-Sponaugle and Jonathan Lazar, Towson University, USA, analyses the ethics of Web accessibility and argues that it is ethical to provide access for the disabled and unethical to exclude them. The authors suggest that the general population would also benefit from more accessible Web pages.

Chapter VI: *Internet Voting: Beyond Technology* by Trisha Woolley and Craig Fisher, Marist College, USA, discusses the issues of privacy, security, authentication and access associated with Internet voting and concludes that its benefits are currently outweighed by negative factors.

Chapter VII: *Protection of Minors from Harmful Internet Content* by Geoffrey A. Sandy, Victoria University, Melbourne, Australia, addresses the problem of how to protect minors from Internet material perceived as harmful without violating adults' right to free speech. The chapter provides a critique of Australia's regulatory framework.

Chapter VIII: *Mobile Communities and the "Generation that Beeps and Hums"* by Marian Quigley, Monash University, Berwick, Australia, argues that, at a time when critics are debating the demise of community, young people today are utilising mobile phones — alone or in combination with the Internet — to establish and maintain mobile, peer-based, social networks.

Part II: Information Security

Chapter IX: *Insights from Y2K and 9/11 for Enhancing IT Security* by Laura Lally, Hofstra University, USA, analyses the Y2K and 9/11 disasters, showing how current Information Technology (IT) infrastructure allows for the propagation of IT threats. The chapter also analyses the efficacy of available IT tools in identifying potential security threats and in mitigating their impact.

Chapter X: *Cryptography: Deciphering Its Progress* by Leslie Leong and Andrzej T. Jarmoszko, Central Connecticut State University, USA, argues that the increase in cyber-terrorism, hackers and white collar crime highlights the need for a stronger security measure in cryptography.

Chapter XI: *A Method of Assessing Information System Security Controls* by Malcolm R. Pattinson, University of South Australia, Adelaide, Australia, proposes a method for assessing a small business organisation's Information System security, utilising an Australian case study.

Chapter XII: *Information Security Policies in Large Organisations: The Development of a Conceptual Framework to Explore Their Impact* by Neil F. Doherty and Heather Fulford, Loughborough University, UK, focuses on large Information Technology organisations in the UK. It presents a research framework designed to test whether and under what circumstances the adoption of an Internet Service Policy is likely to reduce the incidence of security breaches within large organisations.

Chapter XIII: *Metrics Based Security Assessment* by James E. Goldman and Vaughn R. Christie, Purdue University, USA, addresses the problem faced by organisations that, as a result of the September 2001 attacks on the USA, are investing more resources into security measures at the same time as they are enduring an increasing number and frequency of security breaches. The authors propose a method of measuring an organisation's information security.

Chapter XIV: *The Critical Role of Digital Rights Management Processes in the Context of the Digital Media Management Value Chain* by Margherita Pagani, Bocconi University, Milan, Italy, discusses the implementation of digital rights management by five media companies.

References

Baird, R.M., Ramsower, R., & Rosenbaum, S.E. (Eds.). (2000).*Cyberethics*. Amherst, NY: Prometheus Books.

Day, K. (2003). *Inside the security mind: Making the tough decisions*. Upper Saddle River, NJ: Prentice Hall.

Edgar, S.L. (2003). *Morality and machines: Perspectives on computer ethics* (2nd ed.). Boston: Jones and Bartlett.

Gauntlett, A. (1999). *Net spies: Who's watching you on the Web?* Berkeley, CA: Frog Ltd.

Snow, C.P. (1964). *The two cultures and a second look*. London: Cambridge University Press.

Spinello, R. (2000). *Cyberethics: Morality and law in cyberspace*. Sudbury, MA: Jones and Bartlett.

Spinello, R.A., & Tavani, H.T. (Eds.). (2001). *Readings in CyberEthics*. Boston: Jones and Bartlett.

Williams, R. (1981). Communications technologies and social institutions. In R. Williams (Ed.), *Contact: Human communication and history*. London: Thames and Hudson.