The fifteenth and sixteenth centuries are celebrated for the voyages of discovery that proved the world is round. The eighteenth century saw the first proclamations of universal human rights. The twentieth century’s conquest of space made it possible for a human being to look at our planet from a point not on it, and so to see it, literally, as one world. Now the twenty-first century faces the task of developing a suitable form of government for that single world. It is a daunting moral and intellectual challenge, but one we cannot refuse to take up. The future of the world depends on how well we meet it. (Singer, 2004, p.219)

As the renowned ethicist and academic, Peter Singer points out, what may have once been considered as local or national issues are now understood to be global. For example, the growing understanding that greenhouse gas emissions alter the world climate and affect everyone on the planet has generated international forums to attempt to find global solutions. On an economic level, too, a national disaster, particularly in a first world country, can have a worldwide and long lasting effect—as demonstrated by the US financial crisis of 2007. Similarly, technological development and its uses have global implications. Hence, whilst the contributors to *ICT Ethics and Security in the 21st Century: New Developments and Applications* may primarily focus on national case studies or examples, these too, either explicitly or implicitly, have global significance.

Singer also stresses the need for world governance—a scenario made more relevant and pressing by the borderless nature of the Internet. And of course, global governance requires an underlying, mutually agreed upon and universal code of ethics and legislation. The recent dispute between the Google Corporation and Chinese authorities has illustrated both the difficulties of achieving such a consensus as well as those associated with local or national regulation of the Internet.

*ICT Ethics and Security in the 21st Century: New Developments and Applications* highlights both the ongoing nature of some of the issues discussed in my earlier edited volume (Quigley, 2005), as well as new ethical dilemmas and security challenges posed by the rise of more recent technologies. Contributors to this volume address similar challenges to those of the 2005 text—issues such as the digital divide, threats to privacy and organisational security measures—albeit in differing contexts.

The development of Web 2.0 technologies in particular has refocused longstanding debates concerning issues such as copyright, defamation, privacy, and the protection of minors. However, it is the uses to which technology is put, rather than the technology itself which needs scrutiny. As the creator of the first website, Sir Tim Berners–Lee has noted, “This is humanity which is communicating over the Web, just as it’s communicating over so many other different media … we have to, first of all, make it a universal medium, and secondly we have to work to make sure that it supports the sort of society that we want to build on top of it” (Berners-Lee, 2005).
During the last five years, new technologies have developed at apace and have been taken up by users at breathtaking speed. Web 2.0 technologies have enabled the Internet to become interactive so that the reader/consumer has now also become a writer/producer. This is exemplified by the development of social networking services (SNs) such as MySpace, Twitter and Facebook. Individual computer users now write and upload personal diary entries or blogs for public view and upload their home videos for all to share on YouTube. They may expand their network of ‘friends’ via Facebook or assume a virtual identity for participation in a virtual world such as Second Life or in order to play ‘massively multiplayer online role-playing games’ (MMORPGs) such as the immensely popular World of Warcraft (WoW). Students and researchers may choose to contribute entries as well as consult the online encyclopaedia, Wikipedia.

The speed of the take up rate of these technologies is illustrated by the recent claim made by its founders that in the six years since its inception, the number of Facebook users has grown to 500 million or 1 in 14 of the world’s population. However, access to ICTs is still by no means universal, whilst for those with access, security, and privacy concerns remain. For example, the threat to patients’ privacy is one of the concerns highlighted by researchers in the growing area of e-health.

The need for an ethical education and the acceptance of individual moral responsibility in the proper use of technology is also addressed by a number of contributors to this volume. Trust is an essential element between members of virtual communities and young people in particular need to be educated in the proper use of social networking sites so that no one is subjected to defamation or personal vilification. In addition, methods to address the growing problem of plagiarism amongst student populations should include education concerning copyright as well as technological solutions.

Together with the ethical and security problems concerning online sites which are addressed here, other contributors highlight how the advancements in mobile technologies and the widespread use of mobile phones have opened up their potential as a communication device in emergency situations provided they are properly used-and as a more economical alternative for providing access to health information in developing countries.

The need to maintain and update the security of critical infrastructures upon which essential community services depend, as well as that of computer systems within organisations also comprise a significant section of this text. As the authors note, however, security decisions go hand in hand with ethical choices, and organisations need to establish and abide by a system of ethical codes.

ICT Ethics and Security in the 21st Century: New Developments and Applications brings together a selection of relevant current research being undertaken in this important field of study. It comprises a valuable resource for ICT researchers, educators, students and professionals, and both employers and employees of large organisations searching for resolutions to the everyday ethical and security dilemmas with which we must grapple in our highly globalised and technologised world.

ORGANISATION OF THE BOOK

The book is divided into three sections:

- **Section 1**: Online Ethics (Chapters 1-5)
- **Section 2**: Ethical Concerns in the Handling and Delivery of Health and Safety Information (Chapters 6-8) and
- **Section 3**: Ethics and Security in Organisations (Chapters 9-14).
Section 1: Online Ethics

Chapter 1: ‘Understanding Trust in Virtual Communities: Revisited’ by Qing Zou & Eun G. Park, School of Information Studies, McGill University, Canada. The authors highlight trust and trust building as essential elements in communication within virtual communities, particularly as, unlike traditional communities, they have their own unique characteristics such as anonymity and lack of physical presence. Focusing on social rather than technical aspects of trust, this chapter examines different types of trust and the associated issues and challenges.

Chapter 2: ‘Social Networks and Students’ Ethical Behaviour’ by Lori N. K. Leonard & Tracy S. Manly, University of Tulsa, USA. This chapter focuses on social networking sites in order to examine the changing ethical structure of students when using technology. The authors also suggest ways to teach ethics in light of this change and include a discussion of four classical ethical theories that should be considered when discussing or teaching social networking.

Chapter 3: ‘The Ethics of Security of Personal Information upon Facebook’ by Shona Leitch and Matthew Warren, School of Information Systems, Deakin University, Australia. The authors examine the ethical issues associated with personal information as well as the security of that information on social networking systems, with a particular emphasis on Facebook. They discuss a number of examples where personal information has been breached and put forward a model that evaluates the security and risks and proposes a framework that relates to the use of information within Facebook.

Chapter 4: ‘Copyright and Ethical Issues in Emerging Models for the Digital Media Reporting of Sports News in Australia’ by Mary Wyburn, University of Sydney, Australia. This chapter addresses the copyright and ethical issues concerning the emerging models for the digital reporting of sports news in Australia. It also highlights their wider international implications. In particular, it explores the use by news organisations of a defence in copyright law that provides protection against an infringement action for the reporting of news and the use by sports organisations of journalist accreditation to limit, by way of contract, the uses made of copyright material generated at sports events.

Chapter 5: ‘The Protocols of Privileged Information Handling in an E-Health Context: Australia’ by Dr Juanita Fernando, Medicine, Nursing & Health Sciences, Monash University, Australia. Utilizing the findings from two case studies, the author emphasizes the need for a review by health authorities of real-life workplace privacy and security before setting new privileged information handling protocols as the foundation of a new national e-health scheme.

Section 2: Ethical Concerns in the Handling and Delivery of Health and Safety Information

Chapter 6: ‘The Changing World of ICT and Health: Crossing the Digital Divide’ by Prajesh Chhanabhai & Alec Holt, University of Otago, New Zealand. The authors argue that, whilst technology has empowered the healthcare consumer, at the same time, it has contributed to the widening of the digital divide. This chapter examines how developing countries have tackled this problem by using varying communication techniques to share health information. The authors suggest that mobile phone technology may provide better access to health information than the Internet in these countries.

Chapter 7: ‘The Socio-Ethical Considerations Surrounding Government Mandated Location-Based Services during Emergencies: An Australian Case Study’ by Anas Aloudat and Katina Michael, School of Information Systems and Technology, University of Wollongong, Australia. The chapter presents a case
study on how modern technologies, namely mobile applications, are changing the landscape of emergency management in Australia. Through an examination of the 2009 Victorian bushfires, the authors discuss the ethical considerations associated with the adoption of mobile technologies for emergency management.

Chapter 8: ‘Monitoring Employee Actions in the Workplace: Good Business Practice or Unethical Behaviour?’ by Cliona McParland & Dr. Regina Connolly, Dublin City University, Ireland. This chapter examines some of the major issues concerning workplace surveillance in a computer-mediated work environment, including managers’ motivations and employee concerns about threats to their privacy. The ethical impact of monitoring in the workplace is examined, addressing whether management’s ability to monitor employee actions in the workplace represents good business practice or constitutes an invasion of privacy.

Section 3: Ethics and Security in Organisations

Chapter 9: ‘Policy and Issues in Deploying Automated Plagiarism Detection Systems in Academic Communities: A Case Study of Veriguide’ by Chi Hong Cheong, Tak Pang Lau, and Irwin King, Department of Computer Science and Engineering, The Chinese University of Hong Kong.

The authors note that as the Internet has contributed to a growth in student plagiarism, educational institutions are seeking technological solutions to combat it. The chapter examines the policy and issues encountered by the Chinese University of Hong Kong in its implementation of the automated plagiarism detection system, Veriguide.

Chapter 10: ‘Security and Policies in Organisations’ by Nickolas J. G. Falkner, The University of Adelaide, Australia. In attempting to find a well-established code of ethics that binds the organisation as a whole, the author proposes a hybrid ethical approach that can be adapted to any business—one which is flexible, extensible and practical. The chapter provides a set of case studies and general rules as an ethical basis for the development and implementation of security policies. Teleological, deontological, and virtue-oriented aspects of the ethics surrounding organisational ICT security policy are discussed in order to provide a more theoretical basis for an ethical organisation.

Chapter 11: ‘Critical Infrastructure Protection: An Ethical Choice’ by Graeme Pye and Matthew Warren, Deakin University, Australia and William Hutchinson, Edith Cowan University, Australia. Focusing on Australia and utilising the case study of a community threatened by bushfire, the chapter investigates the ethical choices that arise with regard to managing threats to critical infrastructure systems during times of disaster, which may impinge upon the availability and quality of the resources that critical infrastructure systems supply to the community.

Chapter 12: ‘Effective Infrastructure Protection through Virtualization’ by Dennis C. Guster and Olivia F. Lee, St. Cloud State University, Minnesota, USA. Protection of an organisation’s computer infrastructure in order to maintain continuity of operations involves a number of different concerns, including: managing natural disasters, equipment failure, security breaches, poor data management, inadequate design, and complex/impractical design. The authors argue that the virtualization of hosts offers a better means of protection for computer infrastructure which, as well as being easier to manage, can be easily restored following a natural disaster.

Chapter 13: ‘Firewall Rulebase Management: Tools and Techniques’ by Michael J. Chapple and Aaron Striegel, Department of Computer Science and Engineering, University of Notre Dame, USA and Charles R. Crowell, Department of Psychology, University of Notre Dame, USA. This chapter examines the problem of how to keep the firewall—one of the foundational network components for modern day
computer security-at maximum security effectiveness in the face of changing security threats and enterprise application needs. It provides a general model for the auditing and analysis of installed firewalls and insight for the proactive identification of rules with a high likelihood of becoming orphaned in the future.

Chapter 14: ‘Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework’ by James E. Goldman & Suchit Ahuja, Purdue University, USA. The authors propose an integrated framework comprising Control Objectives for Information Technology (COBIT) and Balanced Scorecard (BSC) frameworks, in conjunction with Systems Security Engineering Capability Maturity Model (SSE-CMM), arguing that it provides a more comprehensive mechanism for strategic information security management: one that is fully aligned with business, IT and information security strategies.

Marian Quigley
August 2010

REFERENCES

