Preface

As information systems use becomes more widespread and more individuals and organizations rely on the Internet as a means of conducting business, it becomes ever more important to assure that the Internet is a place where privacy is protected. Additionally, as organizations rely more on information systems, they become vulnerable to attacks on these precious technologies. These are just some of the ethical issues professionals face when dealing with information systems and emerging technologies. Although often overlooked, ethical decision-making is an important issue for all organizations and individuals in the arena of information technologies. In order to better understand the ethical dilemmas facing professionals and private citizens and appreciate their consequences, researchers, practitioners and academics must have access to the latest thinking and practice concerning ethics and information systems. The following chapters contain the most recent research and practices in defining and applying ethical standards. They cover the spectrum of thinking from applying Kierkegaard’s philosophy to Internet education to appreciating the factors that lead to software piracy. There is something that will benefit everyone concerned with the ethics of information systems.

Chapter 1 entitled, “Internet Privacy: Interpreting Key Issues” by Gurpreet Dhillon and Trevor Moores of the University of Nevada, Las Vegas (USA) systematically identifies major Internet privacy concerns. The chapter’s primary purpose is to identify issues related to maximizing Internet privacy. The authors present various researchers’ definitions of the concept and then proceed to discuss a study they conducted attempting to further understand this concept.

Chapter 2 entitled, “One Size Does Not Fit All: Potential Diseconomies in Global Information Systems” by Gerald Grant of Carleton University (Canada) explains how global information systems may lead to diseconomies of scale. The author discusses the differences in companies as well as the internal and external factors that influence an organization’s technology needs and ability to implement information systems. The author proposes careful scrutiny of costs and associated paradigm changes that a company will undergo to implement new technologies.
Chapter 3 entitled, “Some Internet and E-Commerce Legal Perspectives Impacting the End User” by Peter Mykytyn of Southern Illinois University (USA) discusses two legal issues that can confront today’s end users as they do business over the Web. The author addresses the important issues of contract law and jurisdictional issues. These important issues are becoming ever more significant because the current laws were enacted in a world where goods and services were the primary commodities of business, not information.

Chapter 4 entitled, “A New Approach to Evaluating Business Ethics: An Artificial Neural Networks Application” by Mo Adam Mahmood, Gary Sullivan and Ray-Lin Tung of the University of Texas, El Paso (USA) presents a new approach to classifying, categorizing, and analyzing ethical decision situations. The chapter offers a comparative analysis of artificial neural networks, multiple discriminate analysis and chance. This analysis shows that artificial neural networks predict better in both training and testing phases and offer a promising alternative to traditional analytical tools.

Chapter 5 entitled, “Copyright, Piracy, Privacy and Security Issues: Acceptable or Unacceptable Actions for End Users?” by Jennifer Kreie and Timothy Paul Cronan of the University of Arkansas (USA) examines factors that may influence decision-making based upon models of ethical behavior. The results of an empirical study conducted to determine end user perceptions of acceptable or unacceptable behavior and which factors influenced a person’s judgment of the acceptability of a behavior are reported in this chapter. The results reported indicate that the factors that influenced perceptions were based upon the characteristics of the ethical dilemma.

Chapter 6 entitled, “Ten Lessons that Internet Auction Markets Can Learn from Securities Market Automation” by J. Christopher Westland of Hong Kong University of Science and Technology (Republic of China) explores the automation of three emerging market exchanges: The Commercial Exchange of Santiago, The Moscow Central Stock Exchange and Shanghai’s Stock Exchange and compares Internet models of retailing with the older proprietary networked markets for financial securities.

Chapter 7 entitled, “The Societal Impact of the World Wide Web—Key Challenges for the 21st Century” by Janice Burn of Edith Cowan University (Australia) and Karen Loch of Georgia State University (USA) documents the current state of information technology diffusion and connectivity and the related factors such a population density, cultural attitudes and gross domestic product. The chapter then looks specifically at who the “haves” and the “have-nots” with regards to technology are. Finally, the authors then offer concrete suggestions about how the Internet may be used to bridge the gap between the advantaged and the disadvantaged.
Chapter 8 entitled, “Method Over Mayhem in Managing e-Commerce Risk” by Dieter Fink of Edith Cowan University (Australia) identifies the differences between risk management approaches for older information technology systems and those required for e-commerce. The chapter discusses the benefits and critical success factors for an e-commerce risk management methodology. The authors then recommend a program of research to make risk management more dynamic and interactive particularly for the operational aspects of e-commerce.

Chapter 9 entitled, “Why Do We Do It If We Know It’s Wrong? A Structural Model of Software Piracy” by Darryl Seale of the University of Nevada, Las Vegas (USA) examines the predictors of software piracy, a practice estimated to cost the software industry nearly $11 billion in lost revenue annually. The chapter develops a structural model which suggest that social norms, expertise required, gender and computer usage have direct effects on self-reported piracy. The author discusses the theoretical and practical implications for the design and marketing of software.

Chapter 10 entitled, “Ethical Issues in Software Engineering Revisited” by Ali Salehnia of South Dakota State University and Hassan Pournaghshband of Southern Polytechnic State University (USA) looks at each step in the software engineering process and how these steps affect the reliability and safety of the analysis, design and implementation of software. The authors then examine the ethical aspects of software and systems development.

Chapter 11 entitled, “Cyberspace Ethics and Information Warfare” by Matthew Warren of Deakin University and William Hutchinson of Edith Cowan University (Australia) examines the evolution of information warfare from a group of young individuals, hackers to organized individuals, corporations, government agencies, organized crime and terrorists wreaking havoc in the information age. The chapter looks at specific tactics of information warfare and future trends of these attacks.

Chapter 12 entitled, “A Conversion Regarding Ethics In Information Systems Educational Research” by Mark Campbell Williams of Edith Cowan University (Australia) reflects on the author’s own heuristic and psychologically-oriented self study concerning some ethical improprieties committed during the data collection phase of an information systems educational research program. The chapter reports a self-dialogue concerning the issues of ethics and research and asserts that ethical paradigms are especially important when investigating a new media where acceptable ethical practices have not yet been established.

Chapter 13 entitled, “Software Piracy: Are Robin Hood and Responsibility Denial at Work?” by Susan Harrington of Georgia College and State University (USA) examines the factors that lead to the unethical use of computers. Guided by existing ethical decision-making models, this chapter examines the individual
characters that are underlying causes for persistent abuse. The author reports the results of a study which specifically examined the characteristics of responsibility denial and the Robin Hood Syndrome.

Chapter 14 entitled, “Social Issues in Electronic Commerce: Implications for Policy Makers” by Anastasia Papazafeiropoulou and Athanasia Pouloudi of Brunel University (United Kingdom) examines social issues related to electronic commerce policy-making and presents two fundamental social concerns related to policy-making: trust and digital democracy. The chapter then discusses these concerns as they relate to the policy issues concerning network technologies and presents the implications of these concerns for policy-making in electronic commerce.

Chapter 15 entitled, “Kierkegaard and the Internet: The Role and Formation of Community in Education” by Andrew Ward of the University of Minnesota and Brian Prosser of Fordham University (USA) applies Kierkegaard’s philosophy to Internet technologies. The author looks at the effect of communication via the Internet and analyzes the emergence of virtual classrooms in the contest of Kierkegaard’s philosophies.

Chapter 16 entitled, “Manufacturing Social Responsibility Benchmarks in the Competitive Intelligence Age” by James Orton of the University of Nevada, Las Vegas (USA) explores the emergence of social responsibility benchmarks in the competitive intelligence age. The chapter reports on attempts by competitive intelligence agents in the United States and France to manufacture social responsibility benchmarks in the context of covert operations, competitive strategy, corporate intelligence, economic security, economic intelligence and economic warfare.

Chapter 17 entitled, “Strategic and Ethical Issues in Outsourcing Information Technologies” by Randall Reid of the University of Alabama and Mario Pascalev of the Bank of America (USA) identifies major ethical problems and proposes guidelines for ethical conduct in the process of outsourcing information technology. The chapter discusses the benefits and models of outsourcing information technology and looks at ethical literature in general and professional organizations’ codes of ethics in particular. The authors then present and analyze a case study involving IT outsourcing. Finally, the authors suggest general ethical guidelines for outsourcing models.

Chapter 18 entitled, “Ethics, Authenticity and Emancipation in Information Systems Development” by Stephen Probert of Cranfield University (United Kingdom) describes research on the philosophical concept of authenticity used as a framing device for providing an interpretation of ethical and practical action by information systems professionals. The chapter discusses the implications of an IS professional choosing to do research in an authentic manner rather than doing so in adherence with a code of professional ethics or a series of methodological precepts.
Chapter 19 entitled, “On the Role of Human Morality in Information Systems Security: From the Problems of Descriptivism to Non-Descriptive Foundations” by Mikko Siponen of the University of Oulu (Finland) discusses various ethical frameworks and explores objections to the use of ethics as a means of protection based on cultural relativism. The chapter then offers an alternative approach based on a theory of non-descriptivism and discusses the implications of this alternative.

Chapter 20 entitled, “The Government ‘Downunder’ Attempts to Censor the Net” by Geoffrey Sandy of Victoria University (Australia) reports the results of an analysis of the primary sources of an Australian bill, the Broadcasting Services Amendment. The purpose of this bill is to regulate access to content that is offensive to a reasonable adult and unsuitable for children. Specifically, the chapter discusses the important issues that were addressed in the parliamentary hearings and debates. The chapter also comments on the success of the legislation after eight months of operation.

Chapter 21 entitled, “The Genetic Revolution: Ethical Implications for the 21st Century” by Atefeh McCampbell of Florida Institute of Technology and Linda Moorhead Clare of Information Technology Group (USA) defines the practice of DNA analysis and identifies the ethical considerations of human genetic testing in the workplace. The discussion in the chapter is based on a survey conducted to determine the view and level of knowledge among business processional in the workplace on the ethical considerations of genetic testing.

The ethical dimension of information systems encompasses all facets of information technology: research, practice and development. The chapters in this timely new book present theoretical frameworks for developing ethical standards and applying them to information technology research and data analysis. They further discuss practical applications of these frameworks and offer concrete suggestions about how to incorporate ethical thinking into all aspects of organizational life. From legislation censoring the Internet to the threat of information warfare, these chapters are relevant and timely in their understanding and application of the new ethical challenges in the information era.

IRM Press
January 2002