Foreword

We are the first generation of humans where the capabilities of the technologies that support our information processing activities are truly revolutionary and far exceed those of our forefathers. Although this technological revolution has brought us closer and has made our lives easier and more productive, paradoxically, it has also made us more capable of harming one another and more vulnerable to be harmed by each other. Our vulnerabilities are the consequence of our capabilities. Mason (1986) argues that in this age of information, a new form of social contract is needed in order to deal with the potential threats to the information which defines us. Mason states “Our moral imperative is clear. We must ensure that information technology, and the information it handles, are used to enhance the dignity of mankind. To achieve these goals we must formulate a new social contract, one that insures everyone the right to fulfill his or her own human potential” (Mason, 1986, p 26). In light of the Aristotelian notion of the intellect, this new social contract has a profound implication in the way our society views information and the technologies that support them. For Information Technology (IT) to enhance the “human dignity”, it should assist humans in exercising their intellects ethically. But is it possible to achieve this without assuring the trustworthiness of information and the integrity of the technologies we are using? Without security that guarantees the trustworthiness of information and the integrity our technologies, ethical uses of the information cannot be realized. This implies that securing information and its ethical uses are inherently intertwined and should be viewed synergistically. Therefore, we define Information Privacy and Security as an all encompassing term that refers to all activities needed to secure private information and systems that support it in order to facilitate its ethical use.

Until recently, information security was exclusively discussed in terms of mitigating risks associated with data and the organizational and technical infrastructure that supported it. With the emergence of the new paradigm in information technology, the role of information security and ethics has evolved. As Information Technology and the Internet become more and more ubiquitous and pervasive in our daily lives, a more thorough understanding of issues and concerns over the information privacy and security is becoming one of the hottest trends in the whirlwind of research and practice of information technology. This is chiefly due to the recognition that whilst advances in information technology have made it possible for generation, collection, storage, processing and transmission of data at a staggering rate from various sources by government, organizations and other groups for a variety of purposes, concerns over security of what is collected and the potential harm from personal privacy violations resulting from their unethical uses have also skyrocketed. Therefore, understanding of pertinent issues in information security and ethics vis-à-vis technical, theoretical, managerial and regulatory aspects of generation, collection, storage, processing, transmission and ultimately use of information are becoming increasingly important to researchers and industry practitioners alike. Information privacy and security has been viewed as one of the foremost areas of concern and interest by academic researchers and industry practitioners from diverse fields such as engineering, computer science, information systems, and management. Recent
studies of major areas of interest for IT researchers and professionals point to information security and privacy as one of the most pertinent.

We have entered an exciting period of unparalleled interest and growth in research and practice of all aspects of information security and ethics. *Information privacy and security* is the top IT priority facing organizations. According to the 18th Annual Top Technology Initiatives survey produced by the American Institute of Certified Public Accountants (AICPA, 2007) information security tops the list of ten most important IT priorities. According to the survey results, for the fifth consecutive year, *Information Security* is identified as the technology initiative expected to have the greatest impact in the upcoming year for organizations and is thus ranked as the top IT priority for organizations. Additionally, six out of the top ten technology initiatives discussed in this report are issues related to information security ethics, as are the top four. The interest in all aspects of information security and ethics is also manifested by the recent plethora of books, journal articles, special issues, and conferences in this area. This has resulted in a number of significant advances in technologies, methodologies, theories and practices of information security and ethics. These advances, in turn, have fundamentally altered the landscape of research in a wide variety of disciplines, ranging from information systems, computer science and engineering to social and behavioral sciences and the law. This confirms what information security and ethics professionals and researchers have known for a long time that information security and ethics is not just a “technology” issue any more. It impacts and permeates almost all aspects of business and the economy.

In this book, we will introduce the topic of information security and privacy and discuss fundamental concepts and theories from a technical, organizational and ethical point of view. We will broadly discuss tools and technologies used in achieving the goals of information security and privacy. We will consider the managerial, organizational and societal implications of information security and privacy and conclude by discussing a number of future developments and activities in information security and privacy on the horizon that we think will have an impact on this field. Our aim in developing this book is not to present an exhaustive literature review of the research in information security and privacy, nor is it intended to be a comprehensive introduction to the field. Our main goal here is to describe the broad outlines of the field and provide a basic understanding of the most salient issues for researchers and practitioners. This book is presented in six sections. In each section, we aim to provide a broad discussion of an important issue in information privacy and security.

*Hamid R. Nemati*

*The University of North Carolina at Greensboro, USA*