Preface

The last decade of the 20th century was the decade of the Internet. The invention of the World Wide Web (Web) by Tim Berners-Lee, who built the first Web site in 1991 while working at the European Organization for Nuclear Research (or CERN) in Geneva, Switzerland, started a world-wide trend in developing Web sites not only for personal and research purposes, but for disseminating governmental information and for engaging in global electronic commerce. Thus the Internet, with its “killer application,” the Web, heralded the furious pace of globalization in the 1990s.

Today, as the Internet and the Web continue their furious growth and global spread, they have filtered down to encompass every aspect of society. Nowadays it is rare to see an aspect of domestic or public life that is not in some way touched by the Internet. This situation is not restricted only to the technologically developed countries, but is becoming increasingly prevalent in developing countries too. As a result, new terms and phrases such as “virtual world,” “cybercrime,” “computer virus,” “data privacy,” “identity theft,” and “data mining” have entered the everyday vocabulary. Debates have ensued on the virtues and vices of the Web and the consequent large scale digitization that it has heralded.

While many have argued that the pace of the growth of the Internet, the Web, e-commerce, and digitization should continue without any curbs or governmental restrictions, others have argued the exact opposite—that these should be actively regulated and controlled through laws both domestic and international. The latter group has argued that unregulated and unmitigated growth of the Web coupled with the current pace of digitization of almost all data belonging to individuals could cause
an erosion of privacy and cause them to become exposed to malware and identity theft. This would, they argue, curb e-commerce and seriously affect global economic development and growth. Indeed, in the 1990s the Internet was considered to be a virtual world that was ungovernable and thus could not fall under the purview of any government. Proponents of this view felt that the users of the Internet would somehow govern themselves and make it into a global vehicle of commerce and information outside of any governmental influence. However, in recent years, realizing the importance of the Internet, governments also have stepped in to flex their muscles in an attempt to gain control of the Internet through regulations and laws. Predictably, increasing government regulation of the Internet has its detractors who believe that certain fundamental rights such as the freedom of expression may be lost if the government controls the Internet.

These developments and trends have, inevitably, led to a four-way tussle: between the public, governmental policy makers, the technology industry, and the businesses that use the technologies. This intersection of politics, law, privacy, and security in the context of computer technology is both sensitive and complex.

As we are all aware, computer viruses, worms, Trojan horses, spy-ware, computer exploits, poorly designed software, inadequate technology laws, politics, and terrorism all have a profound effect on our daily computing operations and habits. Further, new technological innovations such as file-sharing software and location-based tracking tools also have major privacy-related, political, and social implications. In such an environment, various questions arise, such as: Can there be global laws to preserve security? How will such laws affect privacy? What are the politics of security and privacy? What is the role of legal systems in the way privacy is addressed in various nations? What is the connection between privacy and democratization in various countries? How do organizations tackle the issue of privacy? What are the implications of file-sharing software, peer-to-peer systems and instant messaging in autocratic societies? What are the global effects of file sharing? Are there cultural differences that account for differences in perceptions of security and privacy? Does national or regional culture play a role in shaping the political arguments pertaining to security and privacy? If yes, to what extent?

Unfortunately, basic knowledge and understanding of computer security, especially the legal, political and social underpinnings concerning the use of security technologies within organizations and in the society at large is generally lax. There is a general sense that while security has not improved, privacy has been lost. There is concern about the misuse of information by companies and governments. There also is a general sense that the problems are only getting worse—new developments including electronic voting, Radio Frequency Identification (RFID) tags, location-based tracking technologies, and the Digital Millennium Copyright Act (DMCA) only add to the confusion and concern about security and privacy. In ad-
dition, national and international politics play a very important role in shaping the
discourse on privacy and security.

This book aims to provide a window to academics and practitioners to view and
understand the ties that bind computer technology, security, privacy, and politics.
In addition to chapters on the above topics, the book will also include chapters that
delve into emerging lawsuits and cases, global and societal implications, and how
an individual can protect herself from attacks on privacy.

The 14 chapters of this book offer:

- A point-in-time review of the new developments and thought in the field of
  computer security, with a special focus on privacy, law, and politics in a global
  context
- Its implications on people, business, and law
- The evolution of security and privacy laws and their relevance to society,
  individuals, and corporations
- An examination of security and privacy communities: the practitioners of the
  art
- Provide a vision for the future of security and privacy in the context of global
  politics.

The audience for the book would be anyone from advanced-novice to expert in the
fields of security, privacy, law, and politics; academics, technology managers, social,
and political scientists, CIOs, and information security officers.

Organization of the Book

The book is organized into five sections, with a total of 14 chapters. The first section
briefly introduces the notions of security and privacy in a global context, setting the
tone for the rest of the book. In the only chapter (Chapter 1) in this section, Alok
Mishra gives a nice overview of the theme of the book by assessing various issues
related to individual privacy on the Web, growing concerns among the Web users,
technologies employed for collecting and protecting information on the Web, pri-
vacy-enhancing technologies and the legal provisions to curb the Web privacy. This
chapter also provides a detailed discussion on the Platform for Privacy Preferences
(P3P), its structure, present scenario of its implementation, and its future success.

The second section quickly takes the reader into a major aspect of the implement-
ing computer security and personal privacy across various nations—namely pri-
vacy and security laws. In Chapter II, John Thomas traces the development in the United States of legal protections of the right to privacy. The chapter begins with the common law “right to be let alone” in the early 1900s and proceeds through the enactment of the U.S. Patriot Act in 2001 and the National Security Administration’s warrant-less wire tapping program revealed to the public in 2005. It concludes with a discussion of emerging electronic threats to the security of privacy of the public and concomitant challenges to law makers and law enforcers.

In Chapter III, Sushma Mishra and Amita Goyal Chin discuss some of the most significant of the governmental regulations recently mandated of the IT industry and their considerable impact and implications on information technology, both from a technical and managerial perspective. Employing neo institutional theory as the guiding framework for analysis, they suggest that the plethora of regulations being imposed on the IT industry are migrating organizations in the IT industry to conform and implement standardized processes and practices, resulting in the industry wide commoditization of IT.

In Chapter IV, Bernd Carsten Stahl presents the current state of legal protection of privacy in the United Kingdom. He argues that there are different philosophical concepts of privacy that underpin different pieces of legislation and explores what this may mean for the justification of privacy protection. He then speculates on where the future development in this field may be heading.

The third section focuses on emerging privacy technologies, their uses, and implications.

This section starts with Chapter V, discussing a taxonomy of existing data mining techniques, by Madhu Ahluwalia and Aryya Gangopadyay. Their chapter gives a synopsis of the techniques that exist in the area of privacy preserving data mining. Privacy preserving data mining is important because there is a need to develop accurate data mining models without using confidential data items in individual records. In providing a neat categorization of the current algorithms that preserve privacy for major data mining tasks, the authors hope that students, teachers, and researchers can gain an understanding of this vast area and apply the knowledge gained to find new ways of simultaneously preserving privacy and conducting mining.

In Chapter VI, Yue Liu discusses some rational security and privacy concerns about biometric technology. The author gives a critical analysis of the complexities involved in using this technology through rational discussions, technology assessment and case examples.

In Chapter VII, Roger Clarke addresses the multiple issues of threats to privacy through privacy-intrusive technologies, which have led to a widespread distrust of technology, causing e-businesses to under achieve. He then discusses privacy enhancing technologies (PETs), their technical effectiveness and ways by which
several constituencies can harness PETs. Clarke’s chapter thus examines PETs, their application to business needs, and the preparation of a business case for investment in PETs.

The fourth section focuses on how privacy and security are handled in the organizational context. In Chapter VIII, Ian Allison and Craig Strangwick discuss how one small business planned for, and implemented, the security of its data in a new enterprise-wide system. The company’s data was perceived as sensitive and any breach of privacy as commercially critical. From this perspective, the chapter outlines the organizational and technical facets of the policies and practices evidenced. Lessons for other businesses can be drawn from the case by recognizing the need for investments to be made that will address threats in business critical areas.

In Chapter IX, Richard McCarthy and Martin Grossman examine the connection between Privacy, Security and the Enterprise Architecture Framework. Enterprise Architecture is a relatively new concept that has been adopted by large organizations for legal, economic and strategic reasons. It has become a critical component of an overall IT governance program to provide structure and documentation to describe the business processes, information flows, technical infrastructure and organizational management of an information technology organization. The chapter describes two of the most widely used enterprise architecture frameworks (the Zachman Framework and the Federal Enterprise Architecture Framework) and their ability to meet the security and privacy needs of an organization.

In Chapter X, Frederick Ip and Yolande Chan turn to the ever-important business issue of information security in organizations by researching these issues in the context of Canadian financial firms and educational organizations. Taking a resource-based view of the firm, they examine relationships between the following organizational variables. The organization’s appreciation of the strategic value of its knowledge bases, the information systems security resources, the number and nature of security breaches experienced, and the organization’s customer capital and human capital are studied. Relationships between various variables are tested and a managerially-friendly information security model is validated.

The fifth section discusses some important, interesting, emerging topics and issues in the arena of security, privacy and politics. In Chapter XI, Sue Conger comprehensively discusses emerging technologies and emerging privacy issues. With each new technology, new ethical issues emerge that threaten both individual and household privacy. Conger’s chapter investigates issues relating to three emerging technologies—RFID chips, GPS, and smart motes—and the current and future impacts these technologies will have on society.

In Chapter XII, Anza Akram provides a window into the emerging world of tele-democracy in developing countries. Her chapter discusses the effects of informa-
tion and communication technologies on democracy and focuses on the driving forces, citizen and technology, to understand the effects and future implications. The research is based on literature review and uses informative approach to analyze the existing practices in electronic democracy. It inquires the relationship between the theories in communications and democracy, and analyzes the interaction with the citizens from Athenian and the Orwellian perspectives in Politics. It proposes a framework to identify and analyze the driving forces and the issues related to the digital democracy.

In Chapter XIII, Zheng Yan and Silke Holtmanns introduce trust modeling and trust management as a means of managing trust in digital systems. They state that trust has evolved from a social concept to a digital concept, and discuss how trust modeling and management help in designing and implementing a trustworthy digital system, especially in emerging distributed systems.

Finally, in Chapter XIV, Dan Manson brings a pedagogical focus to the theme of the book. His chapter introduces the interrelationships of security, privacy and politics in higher education. University curriculum politics are ingrained through organizational structures that control faculty hiring, retention, tenure, and promotion, and self-governance policy bodies such as academic senates and faculty curriculum committees that control curriculum approval and implementation. Compounding the politics of curriculum are different constructs of security and privacy, with security viewed as a technical issue versus privacy as a legal and organizational issue. Manson believes that multiple disciplines must learn to work together to teach the constantly changing technical, scientific, legal, and administrative security and privacy landscape. While university “ownership” of security and privacy curriculum may create new political challenges, it has the potential to help limit competing faculty, department and program politics.

Editing this book has been an enlightening and thought-provoking experience to me. I hope that you enjoy reading this book, and that your interest in the field of security, privacy and politics are further aroused through reading the varied perspectives presented by the authors of the various chapters.

Ramesh Subramanian
Hamden, Connecticut, USA
December 2007