Preface

Privacy, the right to be left alone, is a fundamental human right. Risks of the contrary—privacy invasion—have increased in significant proportions in a world increasingly turning online. In today's networked world, a fast growing number of users are hopping on and off the Internet superhighways, multiple times everyday—more so than they hop on and off physical expressways. Internet users are also doing more diverse activities online, including browsing, shopping, communicating, chatting, gaming, and even working. With so much online presence, users find themselves, in many situations, divulging information that they would otherwise may not due to privacy concerns. Users may even be wary of getting online because of fear of possible privacy invasion from the many preying eyes on the Internet. The issue is not whether privacy should be protected or not, rather the issue is how it should be protected in the vast online world where information can be intercepted, stolen, quickly transported, shared unknowingly to the user, or even sold for profit. Compared to an offline environment, the Internet enables collection of more information from users cost effectively, sometimes even without their consent. Thus, the Internet poses greater privacy threat for users as their personal information is transmitted over the Internet if an organization does not have a good security mechanism in place. Furthermore, the connectivity of the Internet allows capturing, building, and linking of electronic profiles and behaviors of users.

Online privacy is a multidimensional concept and thus has been addressed in research from a multiplicity of angles, albeit not equally thoroughly. Much research effort has focused on addressing privacy as a technological factor and hence proposed technical solutions to privacy protection. Although this is an important dimension of online privacy, there are equally, if not more, important dimensions, such as context, culture, perceptions, and legislation. Such softer (non-technological) aspects of privacy cannot be understood by only looking at the technological aspects of privacy. The human dimension is as complex and as important for getting a more complete understanding of privacy. At a micro level, not only that individuals have varying requirements for privacy, but the same individual's requirements may change over time or between situational contexts. Response to privacy invasion may be very different between individuals and situational contexts. There may also be a gap between what individuals' desired and actual behaviors in relation to their privacy concerns. Individuals may have more stringent privacy requirements than what their actual online practice reflects. Online privacy researchers offered less coverage to these human factors, but understanding these factors, and many more, is key to gaining a better understanding of online privacy—hence the human relativism.

At a macro level, privacy requirements and response to privacy invasion may vary across cultures, societies, and business situations. Organizational practices of privacy policies and responses to incidents of privacy invasion affect people's perceptions on the current state of privacy, and consequently affect their trust in the organization. People are generally concerned about how personal information is collected, used, and distributed beyond its original purpose and beyond the parties originally involved. Breaches to how their information is collected, used, or shared and response to such breaches directly impact their privacy concerns and their trust. There is still not sufficient empirical evidence to answer many privacy questions at these macro levels, and many human aspects of online privacy in some social and cultural settings have not yet received enough research attention. Consequently, our understanding of the relationships between online privacy and dimensions such as culture, user characteristics, business context, technology use, and education is still limited.

The world is increasingly turning online and there will be no reversal of this trend. To protect the privacy of online users and to consequently achieve the full potential of transacting in an online world, the issue of online privacy needs to be understood from multiple facets. The challenge is to minimize constraints of online dealings without compromising users' privacy. Such delicate balancing cannot be achieved without a broad understanding of online privacy. This book is an attempt to provide such understanding by offering a comprehensive and balanced coverage of the various dimensions of online privacy. Many previously published books either treat privacy as a sub-topic under a broader topic of end-user computing or information systems or focus primarily on technical issues or managerial strategies. Many others focus on end users and offer only introductory material or general guidelines to enhance personal online security and privacy. While this treatment of these important topics of privacy is appropriate for their intended use and audience, it does not allow for a broader and a more extensive examination of online privacy and how it guides practice.

Furthermore, many gaps in privacy, threats, and fraud theories have not yet been filled. The most prominent such gaps include linking privacy theories to other established theories and frameworks in information technology or related disciplines. For example, culture, social, and behavioral issues in privacy have not received enough attention. Research on human aspects as well as empirical assessments of privacy issues are lacking. Research on linking privacy considerations to business practices, educational curriculum development/assessment, and legislative impacts are also scarce. Many studies have focused on technological advancements, such as security protection and cryptography to offer technical tools for privacy protection and for assessing risks of privacy invasion. Although such focus is a must to protect users from these risks, technology is not equivalent to protection. For a protection scheme to work well, both technical and human aspects have to work in harmony. A major goal of this book is to provide a view of privacy that integrates the technical, human, cultural, and legal aspects of online privacy protection as well as risks and threats to privacy invasion.

The book aims for (a) promoting research and practice in various areas of online privacy, threats assessment, and privacy invasion prevention, (b) offering a better understanding on human issues in these areas, and (c) furthering the development of online privacy education and legislation. The book goes beyond introductory coverage and includes contemporary research on the various dimensions of online privacy. It aims to be a reference for professionals, academics, researchers, and practitioners interested in online privacy protection, threats, and prevention mechanisms. The book is the result of research efforts from content experts, and thus it is an essential reference for graduate courses and professional seminars.

There are 19 great chapters in the book, grouped into five sections: (1) background, (2) frameworks and models, (3) empirical assessments, (4) consumer privacy in business, and (5) policies, techniques, and laws for protection.

The background section provides an overview of privacy for those who prefer a short introduction to the subject. In **Chapter I**, Pauxtis and White point out the serious privacy implications of online searches. Search engines can log and stamp each search made by end-users and use that collected data for an assortment of business advantages. In a world where technology gives users many conveniences, one must weigh the benefits of those conveniences against the potential intrusions of personal privacy. Nevertheless, end-users will always use search engines. They will always "Google" something on their mind. The authors conclude that while the vast majority of casual Internet users either do not know Google's data collection policies, or simply do not care, at the end of the day it comes down to the simple fact that we as a society must put our trust into the technological innovations that have become commonplace conveniences.

In **Chapter II**, Angelina and Tarn brought to the forefront the importance of legal protection and privacy awareness and presented a taxonomic view to explore the relationship of the issues, legal protections, and the remedies and risks for not complying with the legal requirements. The authors used two survey studies to reinforce the vital need for a stronger role by the government and business community as well as the privacy awareness from online consumers themselves. The chapter is concluded with a vital call for consumer privacy education and awareness, government and legislators' attention, and timely responses with legislation that protects consumers against those who would misuse the technology.

In **Chapter III**, Sockel and Falk highlighted the gravity of vulnerabilities to privacy in that it is not uncommon for employees to work offsite, at home, or out of a hotel room, often using less than secure Internet connections—dial-up, cable, Internet cafés, libraries, and wireless. The chapter highlights the relationship between vulnerability, threats, and action in what the authors termed "risk triangle." It delves into techniques that are commonly used to thwart attacks and protect individuals' privacy, and discussed how in the age of unrest and terrorism, privacy has grown even more important, as freedoms are compromised for security. The chapter provides an overview of the various vulnerabilities, threats, and actions to ameliorate them.

Section II consists of four chapters that offer frameworks or models to study various privacy issues. In **Chapter IV**, Jansen, Peen, and Jensen turn the attention to the claim that "Most of the current work has focused on technical solutions to anonymous communications and pseudonymous interactions, but, in reality, the majority of privacy violations involve careless management of government IT-systems, inadequate procedures or insecure data storage." The authors introduced a privacy assessment model, called the *Operational Privacy Assessment Model* that includes organizational, operational, and technical factors. The factors can be evaluated in a simple scale so that not only the resulting graphical depiction can be easily created for an IT system, but graphical comparisons across multiple IT systems are also possible. Although their method has been developed in the context of government IT-systems in Europe, they believe that it may also apply to other government systems, non-governmental organisations (NGOs), and large private companies.

In **Chapter V**, Lilien and Bhargava underline the strong relationship between privacy and trust. The authors contend that the role of trust and privacy is as fundamental in computing environments as it is in social systems. The chapter presents this role in online interactions, emphasizing the close relationship between trust and privacy, and shows how one's degree of privacy can be traded for a gain in the level of trust perceived by one's interaction partner. The chapter explores in detail the mechanisms of this core theme of trading privacy for trust. It also presents different trust models, the interplay between trust and privacy, and the metrics for these two related concepts.

In **Chapter VI**, Ha, Coghill, and Maharaj offer an Australian perspective on measures to protect e-consumers' privacy, the current state of e-consumer privacy protection, and discuss policy implications for the protection of e-consumers' privacy. The authors suggest that although privacy protection measures in the form of legislation, guidelines, and codes of practice are available, their effectiveness is limited in alleviating consumers' privacy and security concerns. The authors contend that protection of consumers' personal information also depends on how e-retailers exercise their corporate social responsibility to provide protection to e-consumers.

In **Chapter VII**, Gurung and Jain review the existing literature and analyze the existing online privacy theories, frameworks, and models to understand the variables that are used in the context of online privacy protection. The authors developed an integrative framework to encapsulate the antecedents to online privacy protection behavior.

Section III includes research studies that report empirical findings on various privacy topics. One main reason that online users are wary of providing personal information is because they lack trust in e-businesses' personal information policies and practices. As a result, they exercise several forms of privacy control as a way to protect their personal data online. In **Chapter VIII**, Rea and Chen report survey results of how the two genders differ in their ways to control their private data on the Internet. Findings provide guidelines for e-businesses to adjust their privacy policies and practices to increase information and transactional exchanges.

Discussion on privacy is incomplete without a glimpse into hackers and crackers—the elite corps of computer designers and programmers, according to Schell and Holt in **Chapter IX**. Schell and Holt argue that it is vital that researchers understand the psychological and behavioral composition of network attackers and the social dynamics that they operate within. This understanding can improve our knowledge of cyber intruders and aid in the development of effective techniques and "best practices" to stop them in their tracks. Such techniques can minimize damage to consumer confidence, privacy, and security in e-commerce Web sites and general information-sharing within and across organizations. The authors discuss known demographic and behavioral profiles of hackers and crackers, psychological myths, and truths about those in the computer underground, and how present strategies for dealing with online privacy, security, and trust issues need to be improved.

In **Chapter X**, Hsu adds a perspective from communications to the ongoing debate on online privacy. She examines why online privacy researchers failed to explain why users asserting to have higher privacy concerns still disclose sensitive information. The author argues that this is due to ignoring the social context (what the author terms situational paradigm) in the research on online privacy. The author tries to offer more support for the argument of the situational paradigm from the newly-emerging phenomenon of online photo album Web sites in Taiwan.

Section IV focuses on consumer privacy in business and consists of four chapters. In **Chapter XI**, Chan, Collins, and Movafaghi tackle the issue of online consumer privacy and digital rights management (DRM) systems of protecting digitally stored content. This protection may be accomplished through different strategies or combinations of strategies including: identifying authorized users, identifying genuine content, verifying proof of ownership and purchase, uniquely identifying each copy of the content, preventing content copying, tracking content usage and distribution, and hiding content from unauthorized users. The authors argue that DRM systems may change the business model from a traditional buy-and-own to a pay-per-use, but caution that this may pose great risks to consumers and society as DRM technologies may weaken the rights to privacy, fair use, and threaten the freedom of expression. The chapter discusses the conflict between the rights of content owners and the privacy rights of content users, and explores several DRM techniques and how their use could affect consumer privacy.

In **Chapter XII**, Parker offers views on online privacy from a marketing perspective in the context of consumer marketing. The chapter provides insights into the ways that online privacy has become a balancing act in which the needs of businesses are oftentimes balanced against the needs of consumers. A number of privacy issues that affect the marketing of products and services are presented, along with recommended best practices. The issues discussed include: (1) consumer, marketer, and government perspectives on data collection, ownership and dissemination; (2) online advertising and the use of cookies and spyware; (3) word-of-mouth marketing and the use of blogs, sponsored chat, and bulletin boards; (4) marketing online to children; and (5) privacy issues in social networks and online communities. The chapter represents one of the first analyses of online marketing practices and their associated privacy issues.

In **Chapter XIII**, Li and Zhang offer analysis of online privacy policies of Fortune 100 companies within the context of the four principles (notice, choice, access, and security) of fair information practices. The authors found that 94% of the surveyed companies posted an online privacy policy and 82% of them collect personal information from consumers. The majority of the companies only partially follow the four principles of fair information practices. In particular, organizations fall short in security requirements—only 19% mention that they have taken steps to provide security for information both during transmission and after their sites have received the information. The authors conclude that a well designed privacy policy by itself is not adequate to guarantee privacy protection, effective implementation is as important. Consumer education and awareness are also essential for privacy protection.

In **Chapter XIV,** Chiou, Chen, and Bisset focus attention on the important question of online privacy across cultures by analyzing cultural perceptions on privacy in the United States, Vietnam, Indonesia, and Taiwan. The authors point out clear differences between how personal information is viewed in the United States and Asia. For example, an American in Taiwan might feel suspicious if asked to provide his passport number by a community Web site, while a Taiwanese in the United States might be puzzled and alienated by the fierceness at which people guard their private lives. The authors argue that such differences should be considered in cross-culture online privacy research and legislation. Furthermore, due to the various cultural differences and backgrounds that form privacy perceptions, great care and sensitivity should be taken into consideration when conducting privacy studies across cultures.

Section IV deals with policies, techniques, and laws for privacy protection. In **Chapter XV**, Lancaster and Yen focus on the important linkage between biometric controls and privacy. Biometrics is an application of technology to authenticate users' identities through the measurement of physiological or behavioral patterns, and thus do not suffer from the shortcoming of external authentication techniques that rely on items that can be lost, forgotten, stolen, or duplicated. The authors conclude that, with adequate communication, users are likely to appreciate systems that allow them the ease of use and convenience that biometric systems offer, and hence their use will continue to grow in the future.

In **Chapter XVI**, Erickson discusses the important issue of the tension between openness in government and personal privacy. The trend in the federal legislature has been to continually strengthen the FOIA and openness by reaffirming a presumption that government records should be released unless there is a compelling reason not to. Alternatively, the trend in agency practice and the courts has been toward more privacy, allowing use of certain exemptions in the FOIA to deny records to individuals or organizations seeking them. This balance has been clarified somewhat by legislation on electronic records, agency practice, and a number of court cases suggesting agencies can limit releases to central purpose activities and records not including individually identifiable information. The author also considers the status and vulnerability of confidential business information passed on to governments and the status and vulnerability of government databases concerning individual citizens. The main conclusion of the chapter is that matters remain in flux in the legal aspects of privacy, and regardless of which way the balance tips (openness vs. privacy), more certainty will help government, organizations, and individuals better plan how and when to share their own information resources.

In **Chapter XVII**, O'Mahony and Flaherty discuss the legal framework for consumer and data protection in Europe which seeks to secure the protection of consumers while simultaneously facilitating economic growth in the European Union. The chapter outlines the main sources of law which protect consumers and their privacy, the important provisions in these sources of law and critically analyzes them, and points the gaps and deficiencies in the consumer and data protection legal structures. The authors argue that the creation of these legal rights and legal protections will only stem the misuse of personal data if people know about the law and their rights and know how to access legal protections. Thus, more needs to be done to ensure that citizens of the European Union are equipped with the necessary knowledge to ensure that their personal data is treated with respect and in accordance with law. The authors conclude that more focus needs to be put on ensuring greater compliance with the law, particularly from businesses who have benefited from the free flow of data.

In **Chapter XVIII**, Mika and Tyler provide an overview of the law relating to cybermedicine and telemedicine in terms of data protection and other legal complications related to licensing and a conflict of state laws. The authors examine the laws applicable to Web sites where medical diagnosis or the purchase of medical services (including prescriptions) is available. They discuss how the new methodology of acquiring medical care is at odds with traditional notions of state regulation and how current laws, both federal and state, leave many gaps related to any consumer protections or potential causes of action when privacy is compromised. The authors posit some expert advice for consumers regarding using websites for medical purposes as well as protecting their own privacy. Lastly, the authors advocate a federal law more punitive that HIPAA; one that regulates and protects patient information, medical transactions, and interactions on the Internet and deters violations of patient privacy by mandating significant fines and imprisonment for negligent or criminal and willful violations of that privacy.

In **Chapter XIX**, Tarn and Hamamoto emphasized trans-border differences in the concepts of privacy; namely, that the concept of privacy in Japan is different than that in the western countries. They explained how, after more and more privacy-related problems were revealed by the media, consumers began to pay attention to the protection of their private information, and, in response, the Japanese government enacted legislation to protect consumers and regulate companies' business activities associated with customers' private information. This exposed many weaknesses in companies' privacy protection systems and revealed unethical uses of private data.

We cannot claim perfection of this book on online privacy, a broad and multidimensional concept. Nevertheless, we believe it fills a major gap in the coverage of privacy by providing a comprehensive treatment of the topic. Thus, it provides a single integrated source of information on a multitude of privacy dimensions including technical, human, cultural, personal, and legal aspects. Research on privacy is still evolving and a varied and broad coverage as presented in this book is a valuable reference for researchers, practitioners, professionals, and students.