
The recent rapid growth of the Internet, together with similar increases in computerization, has been accompanied by soaring deployments of e-business applications. Since e-business ultimately depends on the consumption of ordinary citizens, this has led to more and more consumer personal information in the possession of enterprises. This in turn has led to concerns over potential violations of consumer privacy. In response, various governmental jurisdictions have enacted privacy legislation to protect the privacy of consumers. However, legislation is not enough, protective measures must be in place to guard against potential invasions of privacy. For example, internal business systems include human resource management. What measures are needed to avoid inadvertently revealing employee personal information? Similarly, enterprise communication and collaboration include content management and email. How can these be safeguarded against the leakage of consumer personal information? Finally, e-commerce includes Internet buying and selling. What measures are needed here to preserve consumer privacy?

In this special issue of the International Journal of E-Business Research, we offer a scholarly collection of four articles that provide significant new insights into a) the privacy factors for successful e-transactions and how consumers react to the need to protect private information, b) the privacy protection implications for a business associate of a health care provider, and c) the automated assessment of privacy compliance. We are pleased to serve as guest editors for this special issue and express our deep gratitude to the authors for sharing their valuable research. We also thank the reviewers for contributing many insightful suggestions for improvement.
Referring to the first article “Privacy Factors for Successful Ubiquitous Computing,” Little and Briggs present a study of whether or not privacy principles that have been established by industry really reflect the concerns of the ordinary citizen, in the context of ubiquitous computing. Their research goals were to: a) identify the key privacy concerns of users in a ubiquitous computing context and determine if these concerns reflect established privacy principles, b) ascertain whether or not these concerns vary as a function of context, and c) find out if users will have enough confidence in privacy management procedures to hand-over management and administration of their privacy preferences.

Next, the second article “Consumer Responses to the Introduction of Privacy Protection Measures: An Exploratory Research Framework” by Xu presents a research approach with which information privacy can be viewed in terms of three “lenses”, namely information exchange, social contract, and information control. Xu’s research goal is to apply these lenses separately to discuss information privacy as well as explore factors that influence a consumer’s privacy concerns and how he or she responds to the introduction of privacy measures. This article complements the article by Little and Briggs by looking at information privacy through the different lenses and presenting new results for comparison.

Referring to the third article “Business Associates in the National Health Information Network: Implications for Medical Information Privacy”, Szewczak and Snodgrass consider the role of the business associate (e.g. insurance agent, billing agent, consultant) of healthcare providers in the context of the U.S. National Health Information Network, to identify potential threats to an individuals’ medical information privacy. Their research goal is to identify such threats and propose solutions to management challenges presented by the current and future availability of medical information, made possible by the National Health Information Network.

In the fourth and final article “A Model-Based Privacy Compliance Checker”, Pearson and Allison present a system that addresses the need for e-business organizations to comply with a host of privacy legislations, privacy policies, and privacy best practices. Their system models privacy compliance constraints and automatically assesses the extent to which an organization’s particular computing environment is compliant. In addition, the system generates dashboard-style reports that highlight policy failures. Pearson and Allison’s research goal is to focus on the practical aspects of privacy compliance and provide a solution that meets the needs of e-business.

The articles in this issue illustrate some of the current challenges and research areas pertinent to information privacy in e-business, while in many ways also amplifying the many issues that remain to be addressed. One such issue is the lack of privacy related standards of practice that are applicable to e-business. Another is how to gauge the effectiveness of privacy protection technologies so that management can be encouraged to install them. Undoubtedly, new topics will emerge, and shifts in order to focus on personal needs, as well as business, organizational, regulatory and policy requirements will occur. As this happens it becomes increasingly important to understand the issues associated with the inter-play between e-business requirements, privacy requirements, and privacy protection technologies, in order to ensure e-business systems that are privacy-respecting, trusted, sound, adaptable, and evolvable.
George O.M. Yee is an information scientist in the Information Security Group, Institute for Information Technology, National Research Council Canada (NRC). Prior to joining the NRC in late 2001, he spent over 20 years at Bell-Northern Research and Nortel Networks. George received his PhD (electrical engineering), MSc (systems and information science), and BSc (mathematics) from Carleton University, Ottawa, Canada, where he currently contributes as an adjunct research professor. Yee has served as guest editor for the Journal of Computer Security. He is on the editorial review board of several international journals and is a senior member of IEEE, and member of ACM and Professional Engineers Ontario. He was a general co-chair of the 2007 IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS 2007), and was a member of the organizing committees of the 2006 International Conference on Privacy, Security and Trust (PST 2006) and the 2006 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2006). Yee’s research interests include security and privacy for e-services and e-business applications, information security intelligence, and engineering software for security, reliability, and performance.

Larry Korba is a project leader in the Information Security Group of the Institute for Information Technology of the National Research Council of Canada, Ottawa, ON. As a principal research officer, he is currently the research lead in a major R&D project involving the creation of automated compliance technology for privacy. Over the last 8 years he has led several research privacy technology projects involving collaborators in the European Union, Canada and Taiwan. He has published over 150 research papers in a variety of areas, and has given technical talks at many different venues. His research interests include network and application security, privacy protection, computer supported collaborative work and technologies for security intelligence.

Ronggong Song is a research officer in the Information Security Group, Institute for Information Technology, National Research Council Canada (NRC). He joined NRC in middle 2001 and involved several major R&D projects in the Information Security Group. Song received his BSc (mathematics), MEng (computer science), and PhD (information security) from Beijing University of Posts and Telecommunications. He is a senior member of IEEE, member of AIS, and on the editorial review board of several international journals. He was a member of the technical committees of 2006 IEEE International Conference on Multimedia & Expo (ICME 2006) and served as a co-chair of the Multimedia Security Track. Song’s research interests include security, privacy protection and trust management technologies for e-services, such as network security, pseudonym system, and agent-based security and privacy applications.