Preface

Business and political realities make privacy harder:
— Bruce Schneier in “Architecture of Privacy” (Schneier, 2009)

This book arises from the need to ensure that business leaders and others understand the importance of privacy and have the necessary tools to build privacy into their business processes. Why is privacy important to business? Karen Curtis, the former Privacy Commissioner of Australia, claimed in a keynote address that good privacy is good business, and gave a number of compelling reasons in support of her claim (Curtis, 2006). Among her top reasons are that bad privacy can lead to:

1. Damages to brand and reputation
2. Loss of customers and business partners
3. Loss of valuable information to competitors or malicious individuals

Other reasons (Curtis, 2006) include:

- Business pragmatism: providing good privacy will reduce (or at least not increase) the amount of regulation to which businesses must comply.
- Avoiding legal costs and penalties: businesses do not in general like to be involved in litigation as a result of a privacy breach.
- Improved staff morale: an organization that has respect for privacy embedded in its culture will enjoy a happier and more productive work force.
- Corporate social responsibility: leading businesses take this responsibility to heart, operating in a manner that meets or exceeds the ethical, legal, commercial and public expectations that society has of business.

Why are tools needed to build privacy into business processes? As in most endeavors, tools can help, and in an application area where, for example, privacy may be resisted in favor of the fallacious argument of higher profits, tools are needed. Most professionals have heard of the Privacy Impact Assessment (Warren et al., 2008). This is a tool that evaluates the impact to privacy of a proposed change to business practice. Prior to the introduction of this tool, such impacts to privacy were either done in an ineffective way or not even considered.

Tools are built on technology. Privacy tools are built on privacy technology. A well-known example of privacy technology is the Privacy Enhancing Technology (PET). An example of a PET is the AT&T
Privacy Bird (Cranor, Arjula, & Guduru, 2002), which is a browser plug-in that automatically retrieves privacy policies from service providers and compares these with the user’s specified privacy preferences. Another example of privacy technology is privacy-aware access control. PETs and other privacy technologies are described in this work. The typical business may not have the resources to directly work with some of the more technical privacy technologies, but all privacy technologies can be incorporated into privacy tools by businesses that build the tools. The typical business can then directly make use of these tools.

CURRENT SITUATION WITH BUSINESS PROTECTION OF PRIVACY

The current state of privacy protection in business organizations is far from good. In many organizations, privacy protection is non-existent. Consider the serious privacy breaches that have been recently reported in the news, the latest of which at the time of this writing is the “Sony breach.” In this breach (Akkad, 2011), an attacker stole names, addresses, and other personal data belonging to about 77 million Sony PlayStation Network accounts. Consider also, that it is only the more sensational breaches that are reported in the news. There are many breaches that go unreported.

Most businesses today only pay lip service to privacy requirements by making available their privacy policy. Such a policy is useless unless there are foolproof safeguards that ensure that the policy is followed. In the case of e-commerce, it is next to impossible to tell if the privacy policy is followed. For privacy policies that are posted on e-commerce websites, this editor wrote in (Yee, 2006): “Merely the posting of the website’s privacy policy and requesting consumers to read it is tantamount to a joke. It is more a legalistic self-protection action rather than one that has the consumer’s best interest at heart. First of all, most consumers will not bother to read it – who would? - there are many other more pressing (and perhaps more interesting) things to do. Second, and more importantly, the posted provisions do not speak to the consumer’s personal privacy needs, only the provider’s needs. Everyone is different and have different privacy needs. The expectation of one provider policy fitting everyone’s needs is ridiculous.”

It has been 5 years since this was written, and sadly, ensuring that web posted privacy policies are followed has not measurably improved. About the only areas that have improved in the last 5 years are: a) public awareness of the potential loss of their privacy – this puts more pressure on business to protect consumer privacy, b) increasing awareness by business of the need to comply with privacy regulation, but far more awareness is needed, and c) educational programs are producing more security and privacy professionals.

CHALLENGES AND OPPORTUNITIES

In the coming years, the need for privacy protection in business organizations will only increase. In the past, the rapid growth of the Internet, together with increases in computerization, accompanied by soaring deployments of client-related business applications, resulted in more and more consumer personal information in the possession of business organizations. The Internet is still expanding. Computerization and use of client-related business applications are still growing. In fact, these rates of growth may increase as the world’s economies shift from being based on manufacturing to being based on informa-
tion. Some of the challenges and opportunities that lie ahead for ensuring effective privacy protection in business organizations are:

- Business organizations need to be aware of the need to protect privacy, and the consequences of not protecting privacy.
- Business organizations need to be aware of what actions they need to take to protect privacy, including what tools are available, and carry out those actions.
- Protective foolproof measures must be in place to guard against potential privacy breaches, including safeguards for ensuring privacy policy compliance.
- Privacy legislation needs to be reviewed regularly against changing technology and business practices to ensure that they are adequate, and updated if they are not.
- Penalties for privacy breaches need to be sufficient to persuade business organizations to install privacy protective measures.
- Business privacy practices need to be audited on a regular basis. If such practices are found to be inadequate, the business should be required to upgrade them.
- Government privacy commissioners should have their powers increased and their staff expanded, so that they can participate in auditing business privacy practices, and prosecute violators who refuse to comply.

This work addresses the first four points. As an example of the third point on the need for protective foolproof measures, consider that business communication and collaboration include content sharing and email. How can these be safeguarded against the leakage of consumer personal information? As another example, internal business systems comprise workflows that handle and process client personal information. What measures are needed to avoid inadvertently and illegally revealing this information? What standards can be followed to reduce this risk?

ORGANIZATION OF THIS BOOK

This book reports on the latest advances in privacy protection technologies and their application in business organizations. It is organized into 3 Sections and 14 chapters. A brief description of each chapter follows.

I. Privacy Protection Technology Applicable to Business

This section presents a collection of chapters on privacy protection technology that can be applied to business activities.

Chapter 1: “Privacy Enhancing Technologies for Information Control”

This chapter begins by providing background information on the value of personal information and the privacy regulation approaches in use today. It then describes the challenges and market opportunities of Privacy Enhancing Technologies (PETs). A survey of PETs suitable for business organizations is presented, including a study on the Platform for Privacy Preferences (P3P). The chapter concludes with the authors’ conviction of what businesses have to do to promote privacy.
Chapter 2: "User-Centric Privacy Management in Future Network Infrastructure"

This chapter is concerned with Identity Management (IdM). It describes what IdM is, why it is important, and how it can be useful for both users and business organizations. The chapter begins with background and definitions of terminology. It then discusses the general IdM architecture and standards, and overviews a number of existing IdM systems. An analysis of how IdM can be introduced into organizations is given, along with business opportunities arising from IdM.

Chapter 3: “Leveraging Access Control for Privacy Protection: A Survey”

Access control is fundamental for security. Privacy-aware access control is fundamental to privacy protection. This chapter concerns itself with the legal and technical requirements of privacy-aware access control in business environments and provides a study of the proposed solutions in the literature. The latter includes access control models that incorporate privacy policy enforcing features that account for the purpose of the access, privacy obligations, and other contextual constraints.

Chapter 4: “Self-Protecting Access Control: On Mitigating Privacy Violations with Fault Tolerance”

This chapter discusses privacy and access control in a business context and describes how access control models have been extended in recent years to protect privacy on the Web. It considers the advantages of self-protecting Cryptographic Access Control (CAC) models over standard models in privacy enforcement, and postulates that self-protecting CAC schemes need to be supported by fault tolerance. The authors show how this support can be achieved using ideas from the autonomic computing paradigm.

Chapter 5: “Privacy Hash Table”

Protecting anonymity when publishing microdata (data at the individual level such as age and home address) is always a problem due to linking attacks that can identify the individual owner of the data. k-anonymity is a technique that prevents linking attacks by generalizing or suppressing portions of the released microdata so that no individual can be uniquely distinguished from a group of size k. This chapter investigates a practical full-domain generalization model of k-anonymity and presents an efficient privacy hash table structure to compute a minimal k-anonymous solution.


Business processes describe the set of activities that enterprises perform to reach their objectives. Security and privacy are essential elements in competitiveness. This chapter proposes a model-driven approach for the development of secure (and privacy protecting) business processes. The secure processes also provide artifacts, including security artifacts, useful for software development. The proposal is proved in a case study, verifying its pertinence and validity.

This chapter, by the originator of the “Privacy by Design (PbD)” concept, describes the origins and meaning of PbD, and traces its evolution in terms of information technologies, universal principles to guide the design for privacy, and the work of the Information and Privacy Commissioner of Ontario, Canada, in supporting Privacy by Design. The chapter also outlines the recognition for PbD and the challenges ahead.

II. Privacy Protection in Specific Business Domains

This section is a collection of chapters exploring privacy issues and proposing privacy protection techniques in specific business domains.

Chapter 8: “Privacy Considerations for Electronic Health Records”

Electronic Health Record (EHR) systems are powerful tools for both healthcare providers and patients. Unfortunately, EHR systems also result in new threats to patient privacy. The inclusion of medical images in patient records poses unique challenges, since such images may reveal a patient’s identity or medical condition. This chapter gives an overview of EHR systems, and discusses how privacy challenges from EHR systems and medical images may be mitigated, by combining technology, policy, and legislation aimed at reducing the risk of re-identification.

Chapter 9: “Privacy Protection Issues for Healthcare Wellness Clouds”

A wellness cloud is an instance of cloud computing. A wellness cloud is an integrated, interconnected and intelligent collection of healthcare processors processing data from wellness devices, whose purpose is to help users achieve their wellness goals. This chapter describes the issues and solutions surrounding the privacy protection of healthcare data, as the data resides on the devices, as it travels to the cloud, and as it is processed in the cloud and used by analytic services.

Chapter 10: “Ensuring Privacy and Confidentiality in Digital Video Surveillance Systems”

In recent years, video surveillance technology has come into vogue for general law enforcement and public safety. However, such technology raises issues with privacy protection, lawful evidence enforcement, and content confidentiality, among others. This chapter presents an innovative network-based digital video surveillance solution that meets security and privacy requirements, ensuring that the recorded data will be only accessible to a subset of authorities.
Chapter 11: “Protecting Privacy by Secure Computation: Privacy in Social Network Analysis”

Social network analysis (SNA) is becoming an important tool in investigative organizations such as the police. However, privacy legislation often prevents the free sharing of information needed in SNA. This chapter presents two protocols that allow for the selective disclosure of information needed in SNA. The authors have implemented one of the protocols in a commercial enterprise system used in criminal investigations, showing that SNA can be applied in a privacy-preserving manner.

Chapter 12: “A Dynamic Privacy Manager for Compliance in Pervasive Computing”

This chapter presents a model for assisting user decision making with regard to managing privacy risks associated with pervasive computing. The model brings into alignment four aspects: business, regulation, technology, and user behaviour, and is able to achieve compliance with privacy policies within a dynamic and context-aware risk management situation. The authors describe a small middleware implementation of the model along with the outcomes of the implementation.

III. Privacy Related Analyses and Evaluations

This section presents chapters that provide analyses and evaluations on specific privacy situations, namely harm mitigation for a privacy breach, and the sufficiency (or insufficiency) of privacy legislation to cope with technological change.

Chapter 13: “Harm Mitigation from the Release of Personal Identity Information”

This chapter examines various aspects of harm mitigation from the release of personal identity information, using a real life example involving the release of social security numbers, along with names and addresses. Questions dealt with include: What are the harms associated with a data breach of this nature? How can these harms be mitigated? What are, or should be, the costs and consequences to the organization releasing the data? The authors propose the use of a statistical model to estimate the likely financial repercussions for individuals and organizations.

Chapter 14: “Consumer Privacy Protection in the European Union: Legislative Reform Driven by Current Technological Challenges”

Technological change seems always to be ahead of governing legislation. In the case of automated information systems, personal information can be collected from individuals with very little human interaction, raising serious concerns over data privacy. This chapter evaluates whether current EU legislation is sufficient to ensure that future automated information systems will be designed and built to protect privacy. It also discusses the impact of the legislation on business organizations and suggests solutions for enhancing privacy protection from a legal point of view.
CONCLUSION

This book collects together material that addresses the first four points in the Challenges and Opportunities section above. The first point on business awareness of the need to protect privacy is clearly imparted to readers by all chapters, but especially by chapter 13 on the mitigation of harm. The second point on what actions to take to protect privacy is again covered by all chapters, both from a technology point of view (Section I) and a technology applications point of view (Section II). The third point on foolproof measures is covered by all chapters in Sections I and II. The fourth point on regularly reviewing privacy legislation to ensure adequacy is addressed by chapter 14, which provides an assessment of the sufficiency of privacy legislation to cope with ever changing technology. In addition, this book will provide insights and will support professionals concerned with the management of expertise, knowledge, information, and organizational development in different types of business organizations and environments.

The target audience for this book is composed of business professionals and researchers working in the field of privacy protection in various disciplines, e.g. business sciences and management, information and communication sciences, library, education, sociology, computer science, computer engineering, and information technology.

REFERENCES


