Preface

Almost no one realizes exactly how important privacy is in his or her life.
Bruce Schneier in "Secrets and Lies" (Schneier, 2000)

This book arises from the confluence of three recent trends, namely, the growth of the Internet and e-services, the growth of consumer awareness of their lack of privacy, and the spread of privacy legislation enacted by many jurisdictions. The first two trends in part dictate the need for the third trend, but as we will see, privacy legislation was not enacted solely for e-services and also involves non-electronic privacy. Let us examine each of these trends in more detail:

Growth of the Internet and E-Services. The Internet is growing by leaps and bounds as can be seen by the rapidly increasing amounts of information returned by search engines. The search problem faced by Internet users today is not the lack of information from searches, but how to make sense of the realms and realms of information generated by a search. In addition, the Internet is growing from the spread of computer technology in developing countries as well as the harnessing of the Internet for new applications such as healthcare. Accompanying the growth of the Internet has been the availability of a diverse number of e-services. Most consumers are familiar with online banking or online retailing (e.g. Amazon.com) via the Internet. Other Internet-based services such as e-learning (online courses), e-government (online government services such as tax information), and e-health (online medical advice and others) are becoming more common place as well. Before proceeding any further, it is useful to have a common understanding of an e-service. An e-service for the purposes of this book is characterized by the following attributes (Yee & Korba, 2005):

- The service is accessible across the Internet.
- The service is performed by application software (service software) that is owned by a provider (usually a company).
- The provider's service software can make use of the service software of other providers in order to perform its service.

- A provider can have more than one such service.
- The service is consumed by a person or another application accessing the service across the Internet.
- There is usually a fee that the consumer pays the provider for use of the service.
- The consumer has privacy and security preferences for the service that may or may not be followed by the provider.

For example, consider Amazon.com. Its retailing service is accessible across the Internet. The service is performed by application software owned by Amazon.com. Amazon.com makes use of other providers (e.g. Paypal.com) to provide its service. The service is consumed by individual users across the Internet for a fee (which is built into the price of a product). Finally, each user has privacy and security preferences for the service such as not wanting personal contact information to be disclosed to other parties without permission and wanting such information to be stored securely by the provider. These preferences bring us to the next trend.

Growth of Consumer Awareness of Their Lack of Privacy. Everyone who has ever purchased anything from the Internet has had the experience of pausing and wondering if it is “safe” to enter one’s credit card information. This is an example of a consumer becoming aware of his/her possible lack of privacy. Clearly, the more one is exposed to new services on the Internet and the varied personal information that is demanded by these services, the more one wonders whether the personal information that one enters would be kept safe. Other factors also come into play to push this message home. One very important factor is due to frequent news events of break-ins to credit card servers and corporate process errors that result in consumer private records being faxed to total strangers. How can the consumer have any confidence or trust in providers if they keep hearing such events in the news? In fact, studies have shown that the growth of e-commerce would be many times the current rate if consumers could trust their e-service providers, and a key component of mistrust is the lack of privacy. According to Van Slyke, Belanger, and Comunale (2004), worldwide Internet commerce is expected to reach $8.5 trillion in 2005, of which online retail sales is the most evident, with U.S. consumers spending $51.3 billion online in 2001, $72.1 billion in 2002, and a projected $217.8 billion in 2007. However, these authors also report that not all forecasts are as rosy: while total online spending is increasing, per person online spending is quickly declining. The authors indicate that concerns over privacy and trust are among the most important factors that turn an online buyer into a non-buyer. Finally, consumer attention is being focused on their right to privacy from government legislation (third trend). For example, in Canada, federal privacy legislation has forced common consumer service providers such as dentists and eye glass makers to request consumers to sign forms giving the providers permission to collect their private information.

Spread of Privacy Legislation Enacted by Many Jurisdictions. In recent years, more and more jurisdictions have enacted privacy legislation, which as noted above, focuses the consumer on his/her rights to privacy and contributes to consumer privacy awareness. The federal legislation referred to at the end of the paragraph on *Growth of Consumer Awareness of Their Lack of Privacy* is known as the Personal Information Protection and Electronic Documents Act (PIPEDA) (Government of Canada) and contains provisions for provider accountability, identification of the purpose of private data collection, consent of the consumer for data collection, and others. In the European Union (EU), privacy is defined as a human right under Article 8 of the 1950 European Convention of Human Rights and Fundamental Freedoms. The implementation of this Article can be traced to The Directive (European Union Directive). The Directive applies to all sectors of EU public life and is framed in terms of "data subjects" (owners of private data), "data controllers" (entities having control over private data accountable for correct processing and handling of the data), and "data processors" (entities that process private data on behalf of data controllers). The structure of this framework balances the fundamental rights of the data subject against the legitimate interests of data controllers. Privacy protection in the United States is achieved through a patchwork of legislation at the federal and state levels. Privacy legislation is largely sector-based (Banisar, 1999). Of prominent recent interest are privacy laws enacted in the U.S. healthcare sector, as exemplified by the Health Insurance Portability and Accountability Act (HIPAA) (U.S. Government). HIPAA consumer privacy provisions include the right to obtain a copy of one's medical record, the right to make corrections to one's health information, and the right to give or not give one's permission for the use or sharing of one's health information by a service provider. In all cases of privacy legislation described above, the legislation applies to all pertinent activities that an individual may have in daily life involving the exchange of private information and not only to electronic activity.

The confluence of these three trends yields the following conclusions:

- If e-services are to grow and succeed, consumer privacy must be protected.
- E-service providers will need to protect consumer privacy as prescribed by law.
- International e-services will be subject to privacy laws from multiple jurisdictions. There will be a need for international cooperation to ensure that privacy laws are consistent across national boundaries.

This book suggests solutions for the first two points. The third point is a very complex legal and political issue that requires much indepth research. It is outside the scope of this book.

Current Situation With Protection of Electronic Privacy

The current response of e-service providers to the need for consumer privacy has been weak at best. There are essentially two tiers of privacy provisions offered: the first tier is merely the posting of the Web site's privacy policy, while the second tier consists of the use of P3P (Platform for Privacy Preferences Project) (World Wide Web Consortium) technology that allows the automatic checking of a consumer's privacy preferences against the provider's privacy policy. Merely the posting of the Web site'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. Secondly, 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 has different privacy needs. The expectation of one provider policy fitting everyone's needs is ridiculous. The second tier, the use of P3P technology for automatic checking of a consumer's privacy preferences against the provider's policy is not much better. It only solves the problem of the consumer not bothering to read the policy. The problem of possible mismatch between the consumer's privacy preferences and the provider's privacy policy is still present. To solve this latter problem, providers need to implement systems that allow a consumer to negotiate the provider's privacy policy, where it fails to match-up with the consumer's privacy preferences (Yee & Korba, January 2003, May 2003). While we are on the subject of P3P technology, we should also mention the AT&T Privacy Bird (AT&T), which is a user agent in the form of a bird on the user's screen that changes color to signal that a user's privacy preferences are incompatible with a Web site's privacy policy. This is a cute way of promoting P3P technology and makes the technology more attractive to use, but it still does not solve the personal preferences — provider policy matching problem.

In addition to the current problems of consumers expressing their privacy preferences, the other side of the coin has to do with provider follow-up of consumer's privacy preferences. Let us assume that consumers can express privacy preferences to providers. How do consumers know that their preferences will be followed? Currently, most e-service sites do not provide any form of guarantee that they will even honor *their own* privacy policies, let alone the privacy preferences of consumers. Yet, such guarantees are needed to avoid consumer mistrust of e-services.

Finally, there is today a lack of good security to protect consumers' private information while in the possession of providers. Witness the recent news events concerning break-ins at servers holding consumer credit card information, and bank negligence that saw the faxing of customers' private banking records to a total stranger (the bank continued the faxing even after it was told of it!). This lack of security is becoming even more visible to the public eye as the media focuses on high profile uses of private information in sectors such as healthcare. Another blight on security is the possibility of an insider attack which is extremely difficult to defend against. In the healthcare sector, abuse of private health information by insiders is rampant.

Given today's situation with consumer privacy protection, it is an understatement to say that there is much work to be done. Hopefully, this book will supply some of the missing pieces.

Challenges and Opportunities

In discussing challenges and opportunities (C & O) in e-services privacy protection, a logical path to take is to first address C & O that arise from the current situation as described in the previous section. After that, it would be useful to mention any remaining items. C & O arising from the current situation with e-services privacy protection include:

- Negotiation (perhaps automated) mechanisms are needed to allow e-service consumers to negotiate a provider's privacy policy. Some headway is being made in the area of XML-based Web services where languages such as SOAP, WS-Policy (World Wide Web Consortium-1), and XACML (OASIS) provide facilities to capture privacy preferences and build negotiation systems. However, this work towards negotiation systems is still at the research stage.
- Providers need to implement systems (policy conformance systems) that automatically implement the provisions of a consumer's privacy policy (statement of privacy preferences) and provide guarantees that consumer privacy preferences are followed.
- There needs to be better security put in place to protect a consumer's private information while it is in the provider's possession. In particular, there is a need to find better defenses against insider attack.
- Security implementers need to consider other paradigms of privacy protection. For example, it is not always the protection of private information once it has been given away that is the most effective. The other paradigm is not to give away the private information at all and still fulfill the requirements of e-services. A technology that follows the latter paradigm is pseudonym technology. Another example of a paradigm-like shift in thinking is to apply the mechanisms of digital rights protection to privacy rights protection.
- Consumers need to be educated on their privacy rights (e.g. through exposure to privacy legislation) as well as the use of the Internet. Such education will prepare them to formulate effective privacy policies and negotiate them on the Internet.
- Consumers also need to be empowered with tools and techniques to assess privacy risks in order to make the right privacy choices, either in formulating their privacy policies or in negotiation.
- Standards are needed for policy negotiation and conformance systems to promote cross-service development, consistent essential operation, and trust.

Other challenges and opportunities that complement current privacy needs include:

- System implementers need to examine their system's privacy requirements and learn from good examples of privacy architectures that fulfill the requirements and have been published.
- To make progress in privacy technologies, methods and tools are needed to assess one privacy technology against another and to compare privacy technologies in terms of measures of effectiveness.

Organization of This Book

This book reports on the latest advances in privacy protection issues and technologies for e-services. It is organized into three sections and 11 chapters. A brief description of each chapter follows.

Section I: Issues and Challenges

Chapter I discusses privacy from the viewpoint of the consumer of e-services. It provides a foundation for developing approaches to empower users with control over their private information. It proposes a technique for risk management assessment designed to help consumers evaluate a situation to identify and understand potential privacy concerns. The chapter discusses how a consumer can understand exposure risks and how information can be controlled and monitored to mitigate the risks. It also proposes a method for assessing the consumer's value of personal information. In addition, it presents a mechanism for automated negotiation to facilitate fair, private information exchange. The authors believe that these or similar techniques are essential to give consumers of e-services meaningful control over the personal information they release.

Chapter II discusses privacy challenges of Web Services, which are based on a set of XML standards such as Universal Description, Discovery and Integration (UDDI), Web Services Description Language (WSDL), and Simple Object Access Protocol (SOAP). To enable privacy protection for Web service consumers across multiple domains and services, the World Wide Web Consortium (W3C) published a document called "Web Services Architecture (WSA) Requirements" that defines some fundamental privacy requirements for Web services. However, no comprehensive solutions to the various privacy issues have been so far defined. This chapter focuses on privacy technologies by first discussing the main privacy issues in WSA and related protocols. Then, it provides illustrations of the standardization efforts going on in the context of privacy for Web services and proposes different technical approaches to tackle the privacy issues.

Chapter III examines privacy issues in the health sector and how they are handled in the United States and New Zealand. The increased use of the Internet and the latest information technologies such as wireless computing are revolutionizing the healthcare industry by improving services and reducing costs. These advances in technology help to empower individuals to understand and take charge of their healthcare needs. For example, patients can search for healthcare information over the Internet and interact with physicians. However, the same advances in technologies have also heightened privacy awareness. Privacy issues include healthcare Web sites that do not practice the privacy policies they preach, computer break-ins, insider and hacker attacks, temporary and careless employees, virus attacks, human errors, system design faults, and social engineering. The chapter reports from a study using a sample of 20 New Zealand health Web sites.

Chapter IV describes several aspects of electronic privacy such as needs, approaches, challenges, and models. The author's view is that privacy protection, although of interest to many parties such as industry, government, and individuals, is very difficult to achieve since these stakeholders often have conflicting needs and requirements and may even have conflicting understandings of privacy. Therefore, finding one model or one approach to privacy protection that satisfies all these stakeholders is a daunting task. The chapter discusses various aspects of privacy protection, such as the development of privacy policies, the privacy needs of individuals and organizations, the challenges of adopting and coping with privacy policies, the tools and models to support privacy protection in both public and private networks, related laws that protect or constrain privacy, as well as spamming and Internet censorship in the privacy context. The author hopes that understanding these privacy aspects will assist researchers in developing policies and systems that will bring the interests of the different parties into better alignment.

Section II: Privacy Protection From Security Mechanisms and Standards

Chapter V discusses how implementing network and computer security measures can protect the privacy of Internet users. Personally identifiable information is valuable to both clients and businesses alike, and therefore, both are responsible for securing privacy. Clients and businesses need to understand the vulnerabilities, threats, and risks that they face. They need to know what information requires protection and from whom. Businesses in addition need to comprehend the business issues involved in securing data. Privacy protecting security measures need to be a strong mix of technological, physical, procedural, and logical measures where each measure is implemented in overlapping layers. According to the author, privacy solutions must be flexible, meet the objectives and businesses goals, and be revised on a regular basis.

Chapter VI describes the use of pseudonyms, a privacy protection technology that is rising quickly to prominence. Current e-services allow for easy and efficient personal data collection through integration, interconnection, and data mining, since the user's real identity is used. Pseudonym technology with unlinkability, anonymity, and accountability can give the user the ability to control the collection, retention, and distribution of his/her personal information. The chapter explores the challenges, issues, and solutions associated with pseudonym technology for privacy protection in e-services. The chapter describes a general pseudonym system architecture, discusses the relationships between pseudonyms and other privacy technologies, and summarizes pseudonym application requirements. Based on these requirements, the chapter compares a number of existing pseudonym technologies. In addition, the chapter gives an example of a pseudonym application — the use of an e-wallet for e-services.

Chapter VII presents technologies for privacy enforcement (techniques that can be used to ensure that an organization's privacy promises will be kept). It gives an introduction to the current state of privacy enforcement technologies for e-services environments, proposes a comprehensive privacy enforcement architecture, and discusses some issues and challenges related to privacy enforcement solutions. The authors state that the goal of their proposed architecture, aside from bringing together many of the current isolated technologies, is to ensure consistency between the advertised privacy promises and the actual privacy practices of the e-service provider, so that users can have greater confidence that their personal data will be safeguarded as promised.

Chapter VIII presents a tutorial on how two new XML-based technologies, XACML (eXtensible Access Control Markup Language) and SAML (Security Assertion Markup Language), can be used to help protect privacy in e-services. The chapter briefly introduces XML, and then details the privacy features of XACML and SAML. The chapter illustrates concepts with detailed examples. The author hopes that readers will be both informed and intrigued by the possibilities for privacy applications made possible by XML, XACML, and SAML.

Section III: Privacy Protection Architectures and Other Privacy Topics

Chapter IX first describes some driving forces and approaches for developing and deploying a privacy architecture for e-services. It then reviews several architectures that have been proposed or developed for managing privacy. The chapter offers the reader a quick tour of ideas and building blocks for creating privacy-protection enabled e-services and describes several privacy information flow scenarios that can be applied in assessing any e-service privacy architecture. The authors conclude the chapter with a summary of the work covered and a discussion of some outstanding issues in the application of privacy architectures to e-services.

Chapter X proposes a modeling framework for assessing privacy technologies. The main contributions of the framework are to allow the modeling of aspects of privacy and related system concerns (such as security and scalability) in a more comprehensive manner than the dataflow diagrams traditionally used for privacy analysis. The chapter also takes a feature interaction perspective that allows reasoning about conflicts between a service user's *model* of how the service works and the service's *actual* implementation. To demonstrate the framework, the authors illustrate how it can be applied to the analysis of single sign-on solutions such as .Net Passport.

Chapter XI describes how recent privacy legislation in Canada, the European Union, and the United States can be used to define the minimum and necessary content of a personal privacy policy. The authors believe that the use of a personal privacy policy to express an individual's privacy preferences is best-suited for managing consumer privacy in e-commerce. The chapter first motivates the reader with an e-service privacy policy model that explains how personal privacy policies can be used for e-services. It then derives the minimum and necessary (because it is the law) content of a personal privacy policy by examining some key privacy legislation selected from Canada, the European Union, and the United States.

Conclusions

The editor of this book has collected material that addresses most of the challenges and opportunities mentioned. The material ranges from consumer empowerment to assess privacy risks to security technologies needed for privacy protection to systems for privacy policy enforcement, and even methods for assessing privacy technologies. The editor is confident that the reader will find this book invaluable in the domain of e-services privacy protection.

This book is intended for consumers, educators, researchers, designers, and developers who are interested in the protection of consumer privacy for Internet services. Although there are other books on privacy, no other book contains the latest information and deals with the challenges and opportunities of consumer privacy protection as presented here.

References

AT&T. (n.d.). Articles about AT&T Privacy Bird. Retrieved August 26, 2005, from http://www.privacybird.com/news.html

Banisar, D. (1999, September 13). *Privacy and data protection around the world*. 21st International Conference on Privacy and Personal Data Protection.

European Union Directive. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Unofficial text retrieved September 5, 2003, from http://aspe.hhs.gov/datacncl/eudirect.htm

Government of Canada. (n.d.). Personal Information Protection and Electronic Documents Act. Retrieved February 28, 2005, from http://www.privcom.gc.ca/legislation/index_e.asp

OASIS. (n.d.). *OASIS standards and other approved work*. Retrieved August 26, 2005, from http://www.oasis-open.org/specs/index.php#xacmlv2.0

Schneier, B. (2000). *Secrets and lies, digital security in a networked world*. John Wiley & Sons.

U.S. Government. (n.d.). *Office for Civil Rights — HIPAA: Medical privacy — National standards to protect the privacy of personal health information*. Retrieved February 28, 2005, from http://www.hhs.gov/ocr/hipaa/

Van Slyke, C., Belanger, F., & Comunale, C. L. (2004, June). Factors influencing the adoption of Web-based shopping: The impact of trust. *ACM SIGMIS Database, 35*(2).

World Wide Web Consortium. (n.d.). *Platform for Privacy Preferences Project (P3P)*. Retrieved August 26, 2005, from http://www.w3.org/P3P/

World Wide Web Consortium-1. (n.d.). Links to SOAP and WS-Policy descriptions. Retrieved August 26, 2005, from http://www.w3.org/

Yee, G., & Korba, L. (2003, January). Bilateral e-services negotiation under uncertainty. In *Proceedings of the 2003 International Symposium on Applications and the Internet (SAINT2003)*, Orlando, Florida, USA.

Yee, G., & Korba, L. (2003, May). The negotiation of privacy policies in distance education. In *Proceedings of the 14th IRMA International Conference*, Philadelphia, Pennsylvania, USA.

Yee, G., & Korba, L. (2005). Negotiated security policies for e-services and Web services. In *Proceedings of the 2005 IEEE International Conference on Web Services (ICWS 2005)*, Orlando, Florida, USA.