Preface

In an increasingly competitive landscape, recent years have witnessed a large amount of data collected by organizations to assist them with providing quality and personalized services to their customers and to bolster return on investment to the stakeholders. This is more and more becoming a practice that is very much needed to just keep pace with changing and increasing customer expectations. This is raising serious concerns about privacy protection. There are many dimensions to the privacy problem that this situation is creating. The failure around privacy protection can be caused by many factors including accidental disclosure and intentional and deliberate breach by individuals and organizations. In addition to the causal factors, there could be a potentially wide range of impact from identity theft to legal actions to reputational damage. To address these concerns, the issue around data privacy has been approached from various angles including identity protection, privacy-enhancing techniques and technologies, legal frameworks, and security and trust issues. The book covers these areas in four sections: “Legal Aspects,” “Identity Protection,” “Trust and Security,” and “Detection Techniques.”

Data privacy generally refers to the concepts around how much leverage one has on controlling practices used for collecting and using one’s personal information (Stone et al., 1983; Westin, 1967). Even though conceptually it appears to be a phenomenon which should be easy to understand, there are a lot of aspects of data privacy that create ambiguity and confusion. It has been studied and analyzed from various disciplinary angles including economics, sociology, psychology, technology, and legal, amongst others. Hence, it has been mostly agreed that implications of privacy is contingent on the investigative discipline, such as it means individual rights or corporate practices in legal field (Warren & Brandeis, 1890) and means ability to control collection and use in most social sciences including technology-related fields (Culnan, 1993; Westin, 1967).

The available technologies are providing ways for organizations to collect and innovatively use personal information that were not imaginable a decade ago. This is not only helping companies, but it is also helping individuals. However, recent increase in privacy breaches and resulting impacts have shown that the firms are required to ensure adequate privacy protection (Miller & Tucker, 2009). While individuals express their privacy concerns, they are also open to sharing personal information if they perceive economic benefits (Acquisti & Grossklas, 2005; Bennett, 1995). However, their concerns are only validated with due time because of agency problems of adverse selection, where they don’t have complete information on either the protection practices that will be used to safeguard their information or how the information could be used. The onus is on the companies to not only disclose their practices on how they collect and use information but also to provide sufficient protection to the information. Several legal precedents are showing that transparent and reasonable processes also need to be employed to gain an individual’s consent.
The book covers different contemporary dimensions of data privacy. The book is organized into four sections, each focusing on emerging developments in an important aspect of data privacy. The coverage of the book is detailed and provides latest advancements in the data privacy space in areas of law, security, identity protection, and technology. The book can serve as a reference on data privacy, which is undeniably one of the most pressing challenges in the digital world. The book provides insights into how data (personal information) is collected, stored, and used. Each chapter provides an in-depth discussion on most relevant topics on data privacy including cloud computing, emerging data protection laws and their impact, copyright issues, surveillance, identity protection, detection technologies, and trust and security management. The 19 chapters in the book are contributed by leading data privacy researchers and practitioners from around the world. The chapters cover research into issues and problems of privacy protection within organizations, while providing contributions on technological, legal, policy-based, and trust-based approaches for enhancing privacy protection.

**LEGAL ASPECTS**

In wake of the amount of data collected by private companies and government agencies, many countries around the world are adopting data protection laws that are geared towards information privacy protection of collected sensitive data. There have been numerous cases where failure to protect data privacy has led to many lawsuits warranting government investigations and tremendous monetary and reputational losses to companies. The legal protection provided to individuals around data privacy differs vastly around the world. With recent uptick in formulation of privacy laws around world, today over 80 countries and independent territories have adopted comprehensive data protection laws, most notably in Europe. The US has been facing criticism for not adopting a comprehensive information privacy legal framework, but rather supporting limited sectoral laws in few areas (Greenleaf, 2014). The US laws have been focusing on health care (HIPPA) or credit card companies (PCI).

It has been more than four decades since the first national data privacy law called Data Act of 1973 was adopted in 1973 by Sweden. The US did adopt US Privacy Act of 1974, but that was applicable only to federal agencies. Since then, while the U.S. has been relying on sectoral legislation for data privacy protection, the European Union has adopted a rather comprehensive privacy legislative framework.

In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a “safe harbor” framework. The safe harbor—approved by the EU in July 2000—is a way for U.S. companies to comply with European privacy laws (Safe Harbor, 2014).

Despite this, reconciling the trans-Atlantic divide in scope and scale of data privacy laws, is an enormous task since organizations are challenged by efforts that are needed to track changes to and comply with regulations in the domain of information privacy. Examples of one of these changes in legal framework include impacts of Lisbon Treaty on data protection laws in EU and non-EU states, which one of the chapters covers in the book. In addition, 46 US states have data breach notification acts to inform customers of a potential breach so they can take steps to reduce the adverse impact from consequences of security and privacy breaches.

In Chapter 1 titled “Cloud State Surveillance: Dark Octopus Tentacle Clouds from the Atlantic,” Dr. Sylvia Kierkegaard (of International Association of IT Lawyers, Denmark) asserts that cloud computing opens numerous legal, privacy, and security implications, such as copyright, data loss, destruction
of data, identity theft, third-party contractual limitations, e-discovery, risk/insurance allocation, and jurisdictional issues, and discusses the associated legal risks inherent in cloud computing, in particular the international data transfer between the EU and non-EU states.

In Chapter 2, “Data Protection in EU Law after Lisbon: Challenges, Developments, and Limitations,” the author (Dr. Maria Tzanou, Keele University, UK) provides an analysis of the data protection rules in EU law, focusing on the constitutional and legal developments after the entry into force of the Lisbon Treaty. It examines the jurisprudence of the Court of Justice of the EU on data protection issues, including the recent decisions of the Court on metadata retention and the new right to be forgotten. It concludes with a critical comment on the possibilities and limitations of the EU to provide for effective and comprehensive data protection.

In Chapter 3, “File-Sharing of Copyrighted Works, P2P, and the Cloud: Reconciling Copyright and Privacy Rights,” the author (Pedro Pina, Polytechnic Institute of Coimbra, Portugal) studies how increasingly the distinction between public and private is becoming weaker. The chapter analyzes whether the use of tracking software is consistent with personal data protection legislation and investigates extension of the use of levies in order to compensate rightholders for private copies originating from unlawful sources.

In Chapter 4, “Dataveillance in the Workplace: Privacy Threat or Market Imperative?” the author (Regina Connolly, Dublin City University, Ireland) outlines some of the emerging issues relating to workplace surveillance from the employee perspective, as well as the motivation behind management’s decision to employ technologies in order to monitor employees.

In Chapter 5, “Social Engineering Techniques, Password Selection, and Health Care Legislation: A Health Care Setting,” the authors (B. Dawn Medlin, Appalachian State University, USA, and Joseph A. Cazier, Appalachian State University, USA) discuss current security legislation that addresses the security of patient’s health care records, associated social engineering tactics, and issues with passwords.

IDENTITY PROTECTION

In general, identity and access management to information systems lay the foundation for effective security and privacy management. Implementing a privacy-aware identity management system is critical for any organization’s risk management because such systems provide the first layer of defense for most information assets and hence serve as a foundation for privacy protection. These have been long treated as a commonly available and most used Privacy Enhancing Technology (PET). Privacy-Enhancing Technologies (PET) have considered the technological defense against social and legal privacy problems. PETs not only provide tools to manage personal data so that security and privacy requirements are effectively met but also tools manage access to such data. Modern Identity and Access Management systems provide users with the capabilities to control their own individual and group digital identities, which indirectly affect their ability to control access to their information. However, “[most] existing commercially available Identity Management Systems (IMS) do not yet provide privacy-enhancing functionality” (Hansen, et al., 2008, p. 39). The book includes a few chapters in these areas that provide more insights into recent trends and offerings of identity management systems, which are increasingly becoming important for privacy management. With the advent of big data and exploding data available on social networking sites, companies have started to re-focus their efforts on privacy issues by empowering individuals and organizations alike to manage access to their information, which puts more controlling
powers in their hands. Recent evolutionary trend towards user-centric identity management systems have put “individuals in charge of when, where, how, and to whom they disclose their personal information” (Hansen et al., 2008, p. 39).

Along with PETs, practices and principles also play a vital role in privacy protection. One the most widely accepted set of such principles is the Fair Information Practice Principles (FIPPs). These principles lay the foundation for and provide guidance to companies on how to collect, process, store, and disseminate information. There are many variants of these sets of principles adopted by different organizations. For example, Federal Trade Commission (FTC) sets forth four privacy practice principles for protecting personal information, which include:

1. **Transparency:** To ensure that there is a hidden data collection process and also to provide information on collection of personal data, so users can make an informed decision,
2. **Choice:** To give choices on how the collected information will be used,
3. **Information Review and Correction:** To provide the ability to be able to review and if needed correct collected information,
4. **Information Protection:** To require data collecting entities to provide sufficient protection around the data.

In Chapter 6, “Play That Funky Password! Recent Advances in Authentication with Music,” the authors (Marcia Gibson, University of Bedfordshire, UK; Karen Renaud, University of Glasgow, UK; Marc Conrad, University of Bedfordshire, UK; and Carsten Maple, University of Bedfordshire, UK) discuss and present new research in the field of music-based authentication. This chapter incorporates discussion on recent advances in the field of authentication research within the context of a changing threat landscape. A prototype musical password system is presented and a summary of results from online user testing and a lab-based controlled experiment are presented suggesting the importance of “enjoyability” in assessment of recognition-based authentication schemes.

In Chapter 7, “Privacy, Security, and Identity Theft Protection: Advances and Trends,” the authors (Guillermo A. Francia, III, Jacksonville State University, USA; Frances Shannon Hutchinson, ITEL Laboratories, USA; and Xavier Paris Francia, Jacksonville State University, USA) survey recently enacted national and international laws pertaining to identity theft and privacy issues. Further, the chapter discusses the interplay between privacy and security, the various incentives and deterrence for privacy protection, and the prospects for the simulation of the social and behavioral aspects of privacy using agent-based modeling.

In Chapter 8, “Identity Management Systems: Models, Standards, and COTS Offerings,” the authors (Reema Bhatt, State University of New York – Buffalo, USA; Manish Gupta, State University of New York – Buffalo, USA; and Raj Sharman, State University of New York – Buffalo, USA) highlight the importance of IdM systems in protecting today’s highly vulnerable information assets. The chapter establishes an understanding of the frameworks that IdM systems follow while at the same time helping the reader contrast between different IdM architecture models. The latter part of this chapter elaborates on and discusses some of today’s popular IdM solutions.

In Chapter 9, “How Private Is Your Financial Data? Survey of Authentication Methods in Web and Mobile Banking,” the authors (Vidya Mulukutla, State University of New York – Buffalo, USA; Manish Gupta, State University of New York – Buffalo, USA; and H. R. Rao, State University of New York – Buffalo, USA) survey different Web and mobile banking authentication mechanisms while suggesting considerations to follow per situational demands of various threat environments and possible vulnerabilities in the system.
TRUST AND SECURITY

Trust and security issues play vital roles in assurance for privacy protection effectiveness at all levels. Individuals, in the context of privacy, want to ensure that they control what and how information related to them is collected and have the rights to be able to decide what can be collected and how it is used. Trust is important for individuals when they make such decisions. They are also concerned with how the information will be protected from unintentional disclosure to parties from both inside and outside of the organization. Security breaches have been shown to negatively impact reputation, and hence trust, of the victim organization. For corporations, they are concerned with security of the personal information they collect, store, and use for their business sustenance. They need to institute processes and technologies to enforce laws, policies, and standards to secure personal data from unauthorized disclosure. To assist corporations with securing the information and infrastructure, security models and frameworks provide guidance on how to design the security program for most effectiveness and tailor it to meet their requirements. This also lends them credence on their efforts and initiatives. Chapters in the book discuss implementation of ISO 27001 security model and a framework to manage privacy impact assessment. Other relevant topics include security management systems, security and privacy requirements engineering, and trust building.

In Chapter 10, “Security and Privacy Requirements Engineering,” the authors (Nancy R. Mead, Carnegie Mellon University, USA, and Saeed Abu-Nimeh, Damballa Inc., USA) present a SQUARE security requirements approach that integrates privacy requirements into SQUARE to identify privacy risks in addition to security risks. They present a privacy elicitation technique and then combine security risk assessment techniques with privacy risk assessment techniques.

In Chapter 11, “An Information Security Model for Implementing the New ISO 27001,” the author (Margareth Stoll, Italy) presents a holistic information security and data privacy model that fulfills all requirements of ISO/IEC 27001:2013, which was published in October 2013 to promote integration of other extant standards. Details of implementation of the suggested holistic model in several organizations and the case studies results are described. The model enables data privacy and information security to be part of strategic, tactical, and operational business processes while promoting corporate governance.

In Chapter 12, “Health IT: A Framework for Managing Privacy Impact Assessment of Personally Identifiable Data,” the author (Cyril Onwubiko, Research Series Limited, UK) proposes and discusses a framework for conducting privacy impact assessment of Health IT projects. The chapter provides guidance on how to assess privacy risks of both new and in-service projects and discusses lessons learned from managing privacy risks that result from aggregation, collection, sharing, handling, and transportation of personally identifiable information.

In Chapter 13, “Do We Need Security Management Systems for Data Privacy?” the author (Wolfgang Boehm, Technische Universität Darmstadt, Germany) presents possible uses of corporate and security policies for management systems, including privacy management systems, and identifies their potential applications. Furthermore, the chapter presents a field study, which highlights the advantages of management systems in practice. Moreover, this chapter shows how a formal description of an information security management system can be created by means of discrete-event systems theory and how an objective function for management systems can be defined.

In Chapter 14, “Trust and Trust Building of Virtual Communities in the Networked Age,” the authors (Qing Zou, McGill University, Canada, and Eun G. Park, McGill University, Canada) examine the definitions and characteristics of trust in the context of virtual communities and discuss terms relevant
DETECTION TECHNIQUES

A recent survey (Poneman, 2012) done in the healthcare sector shows that 94% of respondent organizations had at least one data breach in last two years. Important and revealing information from the survey was that more than half of the organizations reported little or no confidence in their organization’s ability to detect all data loss or theft. This shows how critical monitoring and detection is in managing data loss and prevention. Failing to detect data breach and ensuing notification can put tremendous burden and loss to companies. Another survey (Javelin, 2013) shows a strong correlation between data breaches and identity theft. The survey shows that individuals who received a data breach notification in 2012 had an identity theft incidence rate of 22.5 percent, which is more than four times the 5.3 percent rate for all adults.

Forty-six states in the US have adopted breach notification laws. Thirty-six of these states require notification to be done on a prioritized basis without unreasonable delay. Similar initiatives in EU (Directive 2002/58/EC and Regulation 611/2013) require that authorities be notified within 24 hours of the detection of the personal data breach (or within 72 hours in some cases). A “personal data breach” is defined by Directive 2002/58/EC as

... a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed in connection with the provision of a publicly available electronic communications service in the community. (DPWP, 2014, pp. 3)

This highlights the importance of timely detection and response to privacy and security breaches to minimize the negative impact and provide early warning signals for potential damages.

In Chapter 16, “Guidance for Selecting Data Collection Mechanisms for Intrusion Detection,” the authors (Ulf Larson, Ericsson AB, Sweden, Erland Jonsson, Chalmers University of Technology, Sweden, and Stefan Lindskog, Karlstad University, Sweden) provide a detailed explanation of generic data collection mechanism components and the interaction with the environment, from initial triggering to output of log data records. The chapter also presents taxonomies of mechanism characteristics and deployment considerations while suggesting guidelines and hints for mechanism selection and deployment.

In Chapter 17, “An Auto-Reclosing-Based Intrusion Detection Technique for Enterprise Networks,” the authors (Nana K. Ampah, Jacobs Engineering Group, USA, and Cajetan M. Akujobi, Prairie View A&M University, USA) propose a new and unique IDS that employs both signature-based and anomaly detection as its analysis strategies and will be able to detect both known and unknown attacks and further isolate them. The proposed IDS uses auto-reclosing technique that is used on long rural power lines.
The authors assert that the IDS method should effectively block SYN-flood attacks, Distributed Denial of Service attacks (DDoS) based on SNY-flood attacks, and help eliminate four out of the five major limitations of existing IDSs and IPSs.

In Chapter 18, “A Dynamic Subspace Anomaly Detection Method Using Generic Algorithm for Streaming Network Data,” the author (Ji Zhang, University of Southern Queensland, Australia) presents a case study of anomaly detection in large and high-dimensional network connection data streams using Stream Projected Outlier deTector (SPOT) technique. The chapter also introduces innovative approaches for training data generation, anomaly classification, false positive reduction, and adoptive detection subspace generation. The experimental results demonstrate that the technique proposed in the chapter is effective and efficient in detecting anomalies from network data streams and outperforms existing anomaly detection methods.

In Chapter 19, “Detecting Botnet Traffic from a Single Host,” the authors (Sebastián García, Universidad Nacional del Centro, Argentina & Czech Technical University, Czech Republic, Alejandro Zunino, Universidad Nacional del Centro, Argentina, and Marcelo Campo, Universidad Nacional del Centro, Argentina) propose a unique method to analyze trends and behavior of one bot alone to detect bots and botnets. They propose to detect bots in the network traffic by analyzing the relationships between flow features in a time window, based on the Expectation-Maximization clustering algorithm. The result of their study is encouraging, showing a true positive error rate of 99.08% with a false positive error rate of 0.7%.

Manish Gupta
State University of New York – Buffalo, USA

REFERENCES


