Chapter 1
Introduction

Sherali Zeadally and Mohamad Badra

1.1 Overview

Over the last decade, we have witnessed a growing interest and increasing investments in technologies, applications, and system communications around the world. Almost every component in our entourage is being completely networked. With so much sensitive data being generated in the digital world, security and privacy continue to be seen as impediments refraining users from widely using these recent technologies and applications. While privacy is relatively easy to manage within simple client/server architecture, it becomes a significant challenge to ensure privacy in the era of Big Data, cloud computing, and smart applications.

Privacy in a Digital, Networked World—Technologies, Implications and Solutions presents state-of-the-art research results from recognized experts on technical, legal, and ethical privacy issues in various technological areas and emerging paradigms. We expect this book to be a valuable, authoritative reference for students, educators, faculty members, researchers, and engineers currently working or interested in the area of privacy spanning various areas including smart cities, smart grids, Big Data, databases, social networks, healthcare, and so on.

S. Zeadally (✉)
University of Kentucky, Lexington, USA
e-mail: szeadally@uky.edu

M. Badra
Zayed University, Dubai, United Arab Emirates
e-mail: mohamad.badra@zu.ac.ae

S. Zeadally and M. Badra (eds.), *Privacy in a Digital, Networked World*,
Computer Communications and Networks,
DOI 10.1007/978-3-319-08470-1_1

1.2 Database Privacy

Chapter 2 on database privacy presents several privacy techniques (such as statistical disclosure control (SDC) methods, anonymization methods, or sanitization methods) that can be applied to databases. The authors present an overview of the issues in database privacy, a survey of the best-known SDC methods, a discussion on the related data privacy/utility trade-offs and a description of privacy models proposed by the computer science community in recent years. Some relevant freeware packages are also identified. A priori and a posteriori approaches to disclosure control in database privacy sanitization have been reviewed. This chapter looks at sanitization methods, which are common to both approaches, through the discussions on tabular data, queryable databases, and microdata, with a special focus on the latter. Finally, research challenges and opportunities have been identified in the area of statistical disclosure control.

1.3 Privacy and Big Data

Chapter 3 presents a brief review of Big Data technologies, describes the benefits, and outlines how Big Data has come to harm privacy in subtle new forms. The chapter investigates privacy issues that have come up due to technological advancements leading to mostly huge amounts of personal data being stored and communicated. The chapter then reviews the legal and technological issues and describes some possible solutions. It further discusses many open research problems and challenges related to privacy and Big Data. Moreover, this chapter also covers technology, law, and ethics aspects of Big Data analytics from a non-technical perspective.

1.4 Privacy in Crowdsourced Platforms

An overview of privacy in crowdsourcing platforms is given in Chap. 4, with a focus on platforms (such as the Amazon Mechanical Turk (AMT) platform) that specifically deal with the collection and aggregation of information. This chapter emphasizes the privacy risks in online systems and discusses how these risks apply to crowdsourcing platforms, focusing on the potential for exposing Personally Identifiable Information (PII). These risks are illustrated with an example of a real world attack conducted through a series of survey tasks in AMT. In addition, the chapter provides an overview of solutions that can provide privacy protection in online services in general, and identifies those that could also be applied to crowdsourcing platforms. Furthermore, the chapter includes a specific proposal for a privacy-preserving crowdsourcing platform that relies on obfuscation, and describes the design choices surrounding obfuscation techniques, privacy levels, privacy loss quantification, privacy depletion, cost settings, and utility estimation of workers in crowdsourcing platforms. The chapter describes the implementation details for a prototype of the system and summarizes the challenges that still need to be addressed to enhance the privacy of workers in crowdsourcing platforms.

1.5 Privacy in Healthcare

Privacy of healthcare records has been a major concern for a very long time now. Various legislations have been put in place to ensure the privacy of patients. Chapter 5 discusses a few electronic healthcare systems that can be classified into a variety of systems with their own features and faults. The chapter also presents several privacy concerns related to the storage and transmission of health information, the use of mobile devices and social media, and the use of cloud storage systems in healthcare. Moreover, the chapter discusses the privacy challenges that exist in all of the electronic health systems and solutions to address these challenges in those systems. Finally, the chapter highlights future privacy challenges and opportunities related to the development and deployment of electronic health systems.

1.6 Privacy in Peer-to-Peer Networks

Peer-to-peer (P2P) networks are designed to take advantage of dispersed network resources and enable participants to act as servers or clients; their main characteristics include the direct sharing of resources among users, their self-organization, stability, and autonomy. As with other systems, privacy is a major concern in P2P networks. Chapter 6 on privacy in P2P networks starts with an introduction to P2P networks, their classification, and their characteristics. After presenting a brief overview of P2P networks, the chapter identifies and analyzes the existing privacy issues when using P2P networks and the current privacy solutions that can be used. These solutions include anonymous systems, routing modifications, protection of contents when stored and during transmission, private and split credentials, hidden services, and application configuration and hardening. The chapter further explores the challenges that must be addressed in the future. It also discusses future research directions.

1.7 Privacy in the Cloud

Cloud computing technologies are being deployed and used by many businesses, governments, and organizations and are becoming increasingly popular as they offer access to a wide range of infrastructure resources, very convenient pay-as-you-go service, and low cost computing and storage. However, the advantages of clouds come with increased security and privacy risks. Chapter 7 discusses the need for privacy protection and the confidentiality of data and applications outsourced to the cloud. The authors present an overview of multi-tenancy and other inherent properties of the cloud computing model, as well as the novel attack surfaces and threats to cloud users' privacy. The chapter also discusses existing approaches for protecting privacy, and analyzes the pros and cons of these solutions. Finally, it outlines a list of open problems and issues which need to be further investigated and addressed by researchers in the future.

1.8 Privacy in Vehicular Ad Hoc Networks

Chapter 8 discusses various privacy issues in vehicular ad hoc networks (VANETs). The chapter starts by presenting VANET as a new and promising technology that can enhance road safety and provide the foundation for many possible added value applications and services. The chapter then investigates the various security and privacy concerns associated with this technology. The authors present several approaches aimed at protecting user and vehicle privacy in VANET communications and also include a discussion of current solutions and their limitations. Finally, the chapter discusses a broad range of critical security and privacy challenges currently present in VANETs which should be investigated in future research works.

1.9 Privacy Law and Regulation

Chapter 9 deals with the regulation of personal information disclosure and the privacy of individuals. It provides an overview of the laws and regulations used to regulate privacy in the digital age. This chapter examines the current state of US laws that have a direct or indirect impact on the privacy of individuals. The authors of this chapter consider government surveillance and both the laws that allow it and those aimed at placing restraints on law enforcement activities. This is followed by an analysis of privacy regulation in the European Union. The chapter concludes by examining opportunities for change with respect to privacy laws and regulations.

1.10 Privacy in Mobile Devices

The ubiquitous use of mobile devices for personal communications, and subsequently for almost all types of data transactions, has introduced the next level of privacy problems. Chapter 10 includes a review of on-going efforts aimed at retaining the privacy of users constantly interacting with mobile devices for most of their daily activities. It presents an overview of mobile devices and their related technologies. It also highlights the privacy issues associated with the use of a mobile device and discusses the type of personal data that may be collected by a mobile application and the methods by which this data may leak to third parties that are not directly authorized by the user. The chapter discusses the solutions that can be deployed to mitigate mobile device privacy concerns. Finally, the chapter ends with a discussion on the challenges we currently face in making a mobile device a more privacy-aware sensitive platform.

1.11 Privacy with Biometrics

Chapter 11 discusses the topic of privacy in biometric systems. Biometrics can be a very effective tool to keep us safe and secure, prevent individuals from applying for multiple passports or diving licenses, and keep the bad guys out or under control. However, the fact that we are surrounded by so many biometric sensors does limit our privacy in one way or another. This chapter is mainly concerned with privacy issues and solutions surrounding the use of biometrics for recognizing individuals. It provides an adequate background on biometrics and discusses several privacy concerns and solutions about biometrics. The chapter ends with a discussion of some of the outstanding challenges and opportunities in the area of privacy with biometrics.

1.12 Privacy in Social Networks

Social networks such as Facebook and LinkedIn have gained a lot of popularity in recent years. These networks use a large amount of data that are highly valuable for different purposes. Hence, social networks become a potential vector for attackers to exploit. Chapter 12 focuses on the security attacks and countermeasures used by social networks. Privacy issues and solutions in social networks are discussed and the chapter ends with an outline of some of the privacy challenges in the social networks.

1.13 The Right to Privacy in the Age of Digital Technology

Chapter 13 reviews some of the privacy issues that have arisen as a result of the emergence and proliferation of digital information networks. It presents a brief overview of the threats posed to personal privacy, especially for vulnerable groups such as the consumer or users of social media to better understand the nature and scope of the challenges presented by evolving information technologies such as social networking platforms. The author then analyzes several theories of privacy and justifications for privacy, the right to privacy, and how to protect this right. The chapter concludes by describing both the law and technological tools to secure the privacy rights.

1.14 How to Explore Consumers' Privacy Choices with Behavioral Economics

Chapter 14 describes the tools and the evidence to better understand consumers' privacy behaviors. The tools discussed will be useful to researchers, practitioners, and policy makers in the area of consumer privacy. The author presents interesting results about surveying/testing privacy-related behavior of individuals during electronic communications with a particular focus on e-services. The chapter also outlines the principles of conducting empirical research on consumers' privacy consumption behaviors. Explanation is given as to why experiments rather than surveys or hypothetical choices are needed for delivering valid insights to decision makers. After reviewing the existing empirical evidence about the importance that consumers attach to their privacy, the chapter explains the methodological requirements of valid privacy experiments and offers practical advice for conducting privacy choice experiments. This chapter provides a good insight into privacy-enhancing solutions and policies that meet consumers' needs.

1.15 Techniques, Taxonomy, and Challenges of Privacy Protection in Smart Grid

The deployment of Smart Grid technologies has also raised considerable concerns in data privacy issues of Smart Grid users. Privacy concerns in the Smart Grid environment are mostly related to the collection and use of energy consumption data of Smart Grid users. In this context, Chapter 15 discusses various Smart Grid privacy issues and presents Smart Grid privacy protection architectures and approaches. The authors provide a unique taxonomy of the different privacy protection mechanisms that have been recently proposed in the literature. Various strengths and weaknesses of these privacy solutions are also identified. Finally, the chapter discusses some outstanding challenges that need to be addressed to provide robust and scalable privacy protection solutions to Smart Grid users.

1.16 Location-Based Privacy, Protection, Safety, and Security

One of the major benefits of location-based services (LBS) is their ability to maintain safety and security. But LBS can also result in risks such as the use of LBS for cyber stalking others. To establish the need for LBS regulation, we need to understand that there will always be a trade-off between LBS's benefits and the risks associated with their implementation and adoption. Chapter 16 examines privacy and security issues with respect to LBS and recognizes the need for technological solutions, in addition to commitments and adequate assessments/ considerations at the social and regulatory levels. The authors discuss various solutions that have been recently proposed in the area of location-based privacy and identify the various strengths and weaknesses of these solutions. The chapter concludes with a list of interesting challenges relevant to privacy in LBS and the need for further investigation on issues associated with mobility and location technologies.

We hope you will enjoy reading this book as much as we did!