Chapter 3
A Survey of Methodologies for Protecting Privacy of User Data Within Enterprise Information Infrastructure

Asmita Manna
Jadavpur University, India

Anirban Sengupta
Jadavpur University, India

Chandan Mazumdar
Jadavpur University, India

ABSTRACT

During recent years, especially after the introduction of data protection regulations by different countries, protecting the privacy of user data has become an important research topic. Different threads of information privacy research have emerged, particularly in the areas of eliciting privacy requirements, incorporating privacy by design, performing privacy impact assessments, developing privacy enhancement techniques, implementing those techniques for privacy compliance, verifying privacy compliance, etc. Privacy engineering is integral to all phases of data lifecycle, right from privacy requirement elicitation to compliance verification. This chapter covers a brief survey of notable privacy researches and models proposed for different phases of privacy engineering (i.e., privacy requirement engineering, privacy by design, privacy impact assessment, privacy compliance, and modeling approaches for privacy in enterprise infrastructure). Models and frameworks have been chosen based on the relevance of their applicability in modeling and implementing privacy within an enterprise.

DOI: 10.4018/978-1-7998-5728-0.ch003

INTRODUCTION

Today's enterprises collect and process vast amounts of personal data from customers in order to improve customization and quality of services. This opens up a huge attack surface, making such personal data vulnerable to cybercrime. Increasing numbers of incidents of privacy breaches (Dellinger, 2019; O'Flaherty, 2019) is causing customers to become extremely cautious; they are concerned about whether their personal information is being kept and used properly. As business models are becoming more dependent on personal data, enterprises have realized the importance of protecting data privacy to retain their customer base. Therefore, 'privacy management' has become a popular research topic among computer science researchers. This area of research has gathered momentum, especially after the introduction of the promulgation of the General Data Protection Regulation (GDPR) (Regulation G.D.P., 2016) by the European Union.

Aligning the information infrastructure of an enterprise to the privacy requirements specified in different regulations, the specific business needs of the enterprise itself, or to the specific privacy needs of customers, is a difficult task. This alignment can be achieved only if privacy regulations and requirements are considered early in the system design phase rather than incorporating these in the implementation stage on an ad-hoc basis. Several privacy researchers are attempting to formulate ways of incorporating those regulations within different phases of data lifecycle.

Privacy requirements stem from business and legal requirements, in addition to customers' concerns. Hence, it is important to develop a comprehensive privacy model that can elicit privacy requirements of all stakeholders, find ways to integrate those requirements into the system design, and assess privacy risks with respect to the information infrastructure of the enterprise. It is also equally important to choose an appropriate privacy model and make the enterprise compliant with privacy regulations mandated by legal authorities and with their own business needs.

The first step towards developing such a model is to understand the existing research on different aspects of privacy in the enterprise domain. This chapter aims to provide a brief survey of notable research and models proposed for different phases of privacy engineering.

BACKGROUND

Privacy is often considered as secrecy or confidentiality; but, in reality, it is comprised of protection requirements of several parameters derived from legal aspects, privacy policies and principles, and choices of individuals. Privacy was first defined as the 'right to be left alone' by Samuel Warren and Louis Brandeis in their famous law review article, *The Right to Privacy* (Brandeis & Warren, 1890). As proposed by Pfitzmann and Köhntopp (2001), privacy can be technically defined by seven parameters: confidentiality, integrity, availability, anonymity, unlinkability, undetectability, and unobservability.

The privacy of an individual in an enterprise information system depends on how his or her personal data is managed by the enterprise. Personal data of an individual go through different data lifecycle phases in an enterprise information infrastructure. As privacy is integral to all phases of the data lifecycle, aligning the system development lifecycle (SDLC) with the data lifecycle, by identifying how data is processed during different stages of the SDLC, would help enterprises manage privacy better. Thus far, different models and frameworks have been proposed by researchers for integrating privacy in requirements engineering, system design, impact assessment, system implementation, and compliance