Chapter 10
Challenges to Managing Privacy Impact Assessment of Personally Identifiable Data

Cyril Onwubiko
Research Series Limited, UK

ABSTRACT

The challenges organisations face in managing privacy risks are numerous, and inherently diverse. Traditionally, organisations focused on addressing business and security requirements of a project, but most recently, privacy impact assessment has become an essential part of the risk management regime for most projects. Significant efforts are now directed toward providing appropriate guidance on how to conduct privacy impact assessments. Appropriate assessments of privacy invasive technologies, justification for project, collection and handling of personally identifiable data and compliance to privacy legislations possess enormous challenges to carrying out appropriate privacy impact assessments. In this chapter, guidance on how to assess privacy risks of both new and in-service projects is provided. Further, lessons learned from managing privacy risks of new and in-service projects resulting from aggregation, collection, sharing, handling and transportation of personally identifiable information are discussed.

INTRODUCTION

Today's information and communication systems are complex. They span across enterprise boundaries, and use technologies that traverse geographic boundaries, for example, cloud computing. These networks also use a plethora of technologies and software to implement complex business logics, some of which are inherently privacy-invasive, such as location-based technologies, smart cards, radio frequency identification (RFID) tags, and

DOI: 10.4018/978-1-61350-507-6.ch010

biometrics. While these technologies are exciting to use, they pose significant privacy risks.

Traditionally, risk assessments of projects are carried out primarily on the basis of business and security requirements. Most recently, privacy impact assessment (PIA) has been recommended as an essential project initiation process (UK Information Commissioner's Office, 2009) to assess privacy risks associated with new and existing projects. Privacy impact assessment is used to assess privacy risks that may be associated with a project and to ensure that privacy legislations are not breached, and sensitive personal identifiable data (PID) are not compromised too. Privacy risk assessment is an assessment of risks associated with—failing to comply with state or federal privacy legislation—protecting personal information data of individuals, and satisfying privacy requirements of information systems, that may need to be redesigned or retro-fitted at considerable expense (Educause, 2010). This means that privacy risk assessment should be carried out on all projects to ensure that:

1. they comply with privacy legislations or regulations;
2. they provide adequate safeguards to manage, handle, share, store or transport sensitive personal data or personally identifiable information (PII), and
3. finally, they comply with project-specific information systems' privacy requirements.

Managing privacy risks can be challenging, not because of the numerous issues of concern, but also because each project is unique and utilizes fundamentally different technologies and mechanisms to deliver its own service. While the steps involved in carrying out privacy impact assessment are the same for any project, but each assessment of privacy for any project is different.

A project in this chapter refers to a system, programme or scheme. A project may involve a collection of systems that are used to deliver service for a specific purpose. For example, a census programme is a project whose aim is to count the number of lawful citizens, by checking and verifying their name, age, address and social or religious inclination, of a particular nation. This project may require the use of information communications technology (ICT) systems, people, electronic and manual processes. Another example, EINSTEIN 2 (EINSTEIN 2, 2009) is a United States project for intrusion detection system that monitors the network gateways of government departments and agencies in the United States for unauthorized traffic. This project invloves the use of ICT systems, people and both electronic and manual processes to monitor and collect traffic information. An in-service (existing) project is a programme of work that is already been delivered and in operational use. A new project is a programme of work that is in the initiation stage of the project lifecycle.

There are a good number of sources that provide guidelines for conducting privacy impact assessments as demonstrated by (UK Information Commissioner's Office, 2009; Educause, 2010; Radack S., 2010; Gruteser M., and Grunwald D., 2004; Peirce T., 2009; Abu-Nimeh S. and Mead N. R., 2001); unfortunately, organizations still face difficulty assessing privacy risks associated to new and existing projects. Some of the most common challenges faced by organization are as follows:

1. How to assess appropriately privacy invasive technologies;
2. Justification for project;
3. Difficulty finding privacy experts within own organization;
4. Lack of prescriptive guideline on how to assess privacy risks associated to a project, and how to determine the level of privacy assessments required for a particular project.

In addition, how to appropriately gather and handle personal information data and compliance to privacy regulations and legislations are other