Chapter 10

The Integrated Privacy Model:
Building a Privacy Model in the Business Processes of the Enterprise

Munir Majdalawieh
American University of Sharjah, UAE

ABSTRACT

This paper discusses the challenges that faced in the “DigNet” age in terms of privacy and proposes a framework for privacy protection. This framework is integral in ensuring that personal data protection is impeded part of business processes of any systems that are involved in collecting, disseminating, and accessing an individual’s data. The cooperation and partnership between nations in passing privacy laws is essential and requires some building blocks. In this paper, the author argues that the building blocks should be integrated into the business processes and take into consideration three main domains: governments’ legislation, entity’s policies and procedures, and data protection controls. The proposed conceptual framework helps organizations develop data protection in their business processes, assess the privacy issues in their organization, protect the interests of their customers, increase their value proposition to customers, and make it easier to identify the impact of privacy on their business.

DOI: 10.4018/978-1-4666-0026-3.ch010
INTRODUCTION

In the digital and Internet “DigNet” age, a private, public, not-for-profit organizations, and individuals are utilizing the Internet by interacting with their suppliers, customers/clients (online users) or citizens and in most cases they collect and use the personal data for a variety of purposes. The purposes of processing personal data include, but not limited to, buying or selling goods or services; paying fines; banking services; employment’s services; and even when browsing the Internet. When sensitive personal data (bank records, credit card, religious beliefs, political allegiances, travel records, sexual orientation, health, race, membership of past organizations) are being processed, extra controls must be applied. How to protect privacy rights in the “DigNet” age has been a recurring problem since the inception of the Internet. Clarkson et al. (2009) indicate that individuals in the “DigNet” age are not aware that information about their personal lives and preferences is being collected by Internet companies and other online users without even getting the permission to do so. The online marketers are willing to pay a very high price to those who are willing to sell them such information. Because of these concerns and the possibility of lawsuits based on privacy laws, online businesses post on their web sites a privacy policy statement disclosing how personal data obtained from their online users will be used and how the organization will protect and use their online users personal data. But, is this enough to protect the privacy of individuals? And even more important, is this enough to provide online users with assurance that their personal data is protected? Who can guarantee that an organization is meeting its obligation of protecting the online user’s personal data? The “Privacy Statement” is not static, it may change to adapt new laws or when the organization changes its business structure. In such cases, which policy applies to which online user’s personal data and in which territory?

Pirim et al. (2008) argue that privacy has been empirically studied in the information technology research from an organizational context. They added that from a general individual perspective privacy has not been addressed in relation to Information Technology. Furthermore, privacy has not been researched or investigated from business process management perspective and the current literature has shown lack of a well defined methodology for integrating security and privacy into business processes (Anderson & Rachamadugu, 2008). Privacy has a huge impact on the business survival of all companies conducting business online.

Online users are skeptical when it comes to privacy and the Internet in general and online business in specific. The impact of privacy on online businesses is very significant. Teifke (2003) believes that the impact of the potential loss of privacy takes on a whole new meaning when we look at the issue from the perspective of our individual companies. A 2005 poll conducted by Web Design Directory (2005) indicated that 62 percent of the 1000 adults surveyed are worried their personal data could be stolen online. A joint study by TNS and TRUSTe (2008) found that lack of transparency may factor into privacy concerns that online customers have. Among the 1,015 interviewers, 71 percent of the participants are aware that their browsing information may be collected by a third party for advertising purposes. The percent did not change much for the same survey in 2009 (TNS and TRUSTe). This indicates that the online users are aware of the privacy issues and the challenges that they are facing when conducting business or just browsing on the Internet. As such many online businesses are missing huge amount of growth because they are not giving enough assurance to the online users that their personal data is protected. Teifke (2003) concluded that “protecting privacy is good for the bottom line, and not protecting it could be catastrophic.”