Chapter 1.13
Globalization and Data Privacy:
An Exploratory Study

Robert L. Totterdale
Robert Morris University, USA

ABSTRACT

Global organizations operate in multiple countries and are subject to both local and federal laws in each of the jurisdictions in which they conduct business. The collection, storage, processing, and transfer of data between countries or operating locations are often subject to a multitude of data privacy laws, regulations, and legal systems that are at times in conflict. Companies struggle to have the proper policies, processes, and technologies in place that will allow them to comply with a myriad of laws which are constantly changing. Using an established privacy management framework, this study provides a summary of major data privacy laws in the U.S., Europe, and India, and their implication for businesses. Additionally, in this paper, relationships between age, residence (country), attitudes and awareness of business rules and data privacy laws are explored for 331 business professionals located in the U.S and India.

INTRODUCTION

As companies extend their operations into multiple geographies around the world, the need for understanding and complying with data privacy laws and regulations in a myriad of jurisdictions has become critical to avoid penalties, fines, loss of reputation, and possible imprisonment. Since over 90% of business records today are in electronic form (Morelli, 2007) understanding what types of content must be secured, how long it must be retained, when it should be destroyed, how it should be secured, and what limitations exist for transferring the content both within and between companies has become very complex. This complexity arises because some geographies

DOI: 10.4018/978-1-61350-323-2.ch1.13

have strict laws, others have no or limited laws in place relating to data privacy, and yet others have implemented regulations for only specific types of content, or only to address certain industries or groups (Holder & Grimes, 2007; Perkins & Markel, 2004).

Where data privacy laws do exist, differences have been seen in how data privacy is defined, what is considered to be personally identifiable information, and what obligations a company or individual has to meet the requirements of the law (Barnes, 2006). This is further complicated by the existence of case law, state or municipal law, federal law, or constitutional provisions in each geography that may be applicable to certain aspects of how the information about an individual was captured, transferred, or stored in that geography. Penalties for failure to comply also differ between geographies, with some jurisdictions having little enforcement, while others levy fines and penalties that have been into the millions of dollars (Davies, 2008).

The importance of data privacy to companies is reflected in the literature, and is confirmed by the large number of organizations in the legal, accounting, and consulting fields that provide services, training, and education on the topic. In addition, a number of technology providers offer software, hardware, and network security devices that can play a significant role in meeting compliance needs (Anonymous, 2009a, 2009b; Musthaler, 2008; Totterdale, 2008). However, even with the availability of services and technologies to support compliance along with the implementation of "best practices" in an organization, a partner in a major international law firm argues that "there will always be failures-…." Additionally, Segrio Pedro, a managing director of PWC cites recent survey results from his organization that revealed that "most organizations (54% of respondents) do not know where personal data is collected, transmitted or stored" (Anonymous, 2009d).

This study provides a summary of major data privacy laws in the U.S., Europe, and India. Each of these countries is a major contributor in global commerce or outsourcing services. In addition, through survey research of 331 professionals who were assigned to one of two technology projects located in the U.S. and India, attitudes toward and awareness of business policies and data privacy laws were assessed. The purpose of the analysis was to explore whether differences in attitudes and awareness existed based on the home geography (i.e. country) of the participants, the project team to which they were assigned, their ages, and their frequency of use of electronic content. These differences were explored through the following research questions:

R1. Do awareness and attitudes differ based on project assignment (i.e. Project 1 or 2)?
R2. Do awareness and attitudes differ based on participant ages?
R3. Do awareness and attitudes differ between U.S. and Indian residents?
R4. Do awareness and attitudes differ for frequent users of electronic content versus infrequent users?

The findings from this research provide insights to differences in attitudes and awareness that may be useful in implementing new business practices to improve compliance and/or minimize business risk.

LITERATURE REVIEW AND COMPANY BACKGROUND

The importance of data privacy has long been recognized in law by many countries, states, and municipalities from around the world (Stephens, 2007). However, the various legal systems today are rarely consistent in their definition of terms, the obligations imposed on individuals and organizations, and the remedies for failure to comply with their respective laws (Perkins & Markel, 2004). Significant laws have been implemented, such