Privacy Protection Overseas as Perceived by USA-Based IT Professionals

Jaymeen R. Shah, Texas State University — San Marcos, USA
Garry L. White, Texas State University — San Marcos, USA
James R. Cook, Texas State University — San Marcos, USA

ABSTRACT

Privacy laws for the Internet are difficult to develop and implement domestically and internationally. A clear problem is how such laws are limited to national jurisdictions. What is legal in one country may be illegal in another. Due to differences in cultures and values, and government types, it may not be possible to establish global standards and legislations to ensure privacy. Due to the nonexistence of global privacy standards, multinational (international) companies usually select one of the following two possible solutions: (1) implement a most restrictive “one size fits all” privacy policy that is used across various countries, or (2) implement different privacy policies that meet the privacy regulations of different countries and expectations of those citizens. In order to investigate a solution that may be used by multinational companies, and how companies view domestic privacy laws, the authors conducted a survey of U.S.-based employees of domestic and multinational companies. The results of the survey suggest that the majority of the multinational companies prefer the first solution—most restrictive “one size fits all” approach. They develop and implement a single set of privacy policies that is used across their operations in different countries. The majority of the companies surveyed consider domestic privacy laws in the United States to be practical, but ineffective.

Keywords: e-commerce privacy; global privacy laws; information privacy policies; Internet; laws; policies; privacy

INTRODUCTION

Computer technologies, especially the Internet, have created an electronically connected global community. The Internet and World Wide Web allow easy collection and distribution of information across the globe. Use of the World Wide Web has exponentially increased over the past few years. It is used by businesses as an important sales and communications channel, and by consumers for information research and e-shopping. The free flow of information is one of the most essential requirements for the economic growth of any organization (Oz, 1994).

Information on a Web page can be viewed and accessed from across national and judicial boundaries. Such universal access to Web pages allows businesses to market their products
across the globe using the Web. When consumers shop on the Web, they are required to enter personally identifiable information such as their name, address, and credit card number. This personally identifiable information may be transmitted across the boundaries of states and countries depending upon the locations of the customer and the Web server hosting the Web site. Transmitting data across the globe has become necessary for international business (Oz, 1994). A major issue for global e-traders is privacy (Chandran, Phatak, & Sambharya, 1987; Zuckerman, 2001). Such an issue can threaten the growth of e-commerce. Surveys have indicated that consumers have become concerned about privacy on the Internet, to such an extent, that 61% of the users refuse to shop online (Ryker, Lafleur, Mcmanis, & Cox, 2002).

The Internet has promoted direct interactions between businesses and their customers, irrespective of their locations around the world. There are no immigration or customs checks. Data flows across the globe just as it flows across a local area network. However, this has created a new problem with consumer and employee privacies as existing privacy laws do not seem to adequately address the privacy issues across geographical boundaries. Further, privacy laws across different countries differ (Zuckerman, 2001). For example, in many countries the data is owned by the data collector (e.g., United States), while in other countries, the data is owned by the person concerned (e.g., European Union). Another difference is how the laws govern the operations of law enforcement agencies and telecommunication services. This brings up the question as to how multinational companies deal with and perceive the patchwork of privacy laws that exist across the various countries of their operations. The primary purpose of this research is to answer this question.

We will first discuss the threats to privacy from the increased use of the Internet and e-commerce. Next, we will provide an overview of privacy laws of some countries. This will provide a perspective about the extent to which privacy laws differ across countries around the globe. We then discuss the survey methodology, followed by a discussion of the results of the survey.

THREATS TO PRIVACY

Privacy is defined as the right of an individual or business to determine when, how, and how much information about them should be disclosed to others (Grandinetti, 1996; Martin, 1973; Udo, 2001). The Internet and e-commerce have created potential threats to privacy, which are invisible to most users (Camp, 1999; Pedley, 2002). Although many believe that the Internet is anonymous, the reality is to the contrary. The Internet is shifting away from the assumptions of anonymity upon which it was originally designed (Bennett, 2001). For example, a client computer can be traced via the Internet Protocol (IP) address. The Web server also can place a “cookie” on a client PC, which can be subsequently used to exchange information between the client PC and the Web server. A “cookie” can keep track of user’s online activities, such as Web pages visited, date and time of access, and duration of access. This information about a user’s online activities can be sent back to the Web server. In certain situations, such stealthy monitoring of a user’s online activities can constitute violation of a user’s privacy (Rezgui, Bouguettaya, & Eltoweissy, 2003). When a user enters personal information on a Web page, more privacy issues come into play, especially when accessing a Web server located in another country. Several U.S. federal agency Web sites track users’ online activities despite rules banning the practice (Mearian, 2001). Privacy advocates argue that organizations should ask permission before tracking users’ online activities (Roha, 2000). Users should have the right to prevent some transfers of personally identifiable information (Graham, 1987). This may require that a user be more involved in protecting his/her privacy. For example, a user could block cookies from being placed on their computer. The most recent version of the Internet Explorer browser, allows users to select between receiv-
Related Content

Fundamental Risk Factors in Deploying IT/IS Projects in Omani Government Organisations
[www.igi-global.com/article/fundamental-risk-factors-deploying-projects/3577?camid=4v1a](www.igi-global.com/article/fundamental-risk-factors-deploying-projects/3577?camid=4v1a)

AMERIREAL Corporation: Information Technology and Organizational Performance
[www.igi-global.com/chapter/amerireal-corporation-information-technology-organizational/6303?camid=4v1a](www.igi-global.com/chapter/amerireal-corporation-information-technology-organizational/6303?camid=4v1a)

Leapfrogging an IT Labor Force: Multinational and Indigenous Perspectives
[www.igi-global.com/article/leapfrogging-labor-force/51329?camid=4v1a](www.igi-global.com/article/leapfrogging-labor-force/51329?camid=4v1a)
Establishing the Human Dimension of the Digital Divide
www.igi-global.com/chapter/establishing-human-dimension-digital-divide/19195?camid=4v1a