INFORMATION SCIENCE PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB8199

Chapter V

Information Technology and Privacy: A Boundary Management Perspective

Jeffrey M. Stanton
Syracuse University, USA

ABSTRACT

With the rising popularity of the Internet and some widely publicized occurrences of privacy loss due to information technology, many individuals have recently become more concerned with the privacy and security of sensitive information. These concerns have special relevance within work organizations because of the substantial amounts of data that organizations typically collect about the work and non-work activities of their employees. This chapter presents a new theoretical perspective called Information Boundary Theory, that describes whether, when, and why employees care about the privacy and security of sensitive information at work. Analysis of interview data from N=25 non-managerial U.S. workers provided preliminary support for four of the new theory's research propositions. The chapter describes implications of the theory and the research findings for the design and deployment of information technology systems within organizations and maps a research agenda for future uses of the theory.

INTRODUCTION

The deployment of information technology into organizations has continued to accelerate over recent years. Information technology systems that leverage networks, databases, and telecommunications channels carry, distribute, display, and store an increasing amount of data that has personal relevance to individual

This chapter appears in the book, *Socio-Technical and Human Cognition Elements of Information Systems* edited by Steve Clarke, Elayne Coakes, M. Gordon Hunter and Andrew Wenn.

workers. Thus, designers, administrators, and users of such systems may have a strong interest in facilitating and assuring proper regulation of personal information flows. From a technical standpoint such matters are handled through a variety of mechanisms such as encryption and access control, but from a social standpoint, it is important to understand what information must be protected, when, and why. In this chapter I synthesize a framework for understanding the regulation of personal information flows based on three component theories relevant to the privacy of personal and performance information in organizational settings. This framework, called information boundary theory, uses a guiding metaphor from psychologically grounded research on communications boundary management. In support of the viability of the framework, I discuss qualitative data from an interview study that provided a preliminary assessment of the framework. Finally, I discuss applications of the framework to future research and to the practice of information systems design.

INFORMATION TECHNOLOGY AND PRIVACY: A BOUNDARY MANAGEMENT PERSPECTIVE

Commercial, non-profit, and governmental organizations use information technology in a variety of ways to obtain and communicate data about their employees, clients, customers, and other relevant individuals. While this observation has been true for many years, key issues such as privacy have become particularly salient with the widespread availability of new data collection, transmission, and storage strategies facilitated by the Internet, intranets, databases, and related information technologies (see, for example, Agre, 1997; Kahin & Nesson, 1997, p. x; U.S. Congress, 2000). In parallel to these developments, increased use of telecommunications media to support the quotidian communications needs of organizations has resulted in a consequent increase in the transmission of sensitive personal information through such channels as email, voicemail, and instant messaging. Investigations of these issues have clearly shown that organizations and their members must take special care in regulating the flow of personal information through the wide variety of information technology systems available now and in the future (Eddy, Stone & Stone-Romero, 1999; Pincus and Trotter, 1995; Sipior, Ward, & Rainone, 1998; Stanton & Weiss, 2000).

From a purely technical standpoint, specific remedies to ensure the security of data (e.g., authentication, access control, encryption, etc.) have long been available, and researchers continue to expand and enhance the repertoire of available techniques. From a socio-technical point of view, however, these techniques comprise a toolbox; the difficult work lies in knowing when a particular tool is