IGI PUBLISHING **ITJ4225**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Information Security and Privacy, Volume 2, Issue 2
edited by **Hamid R. Nemati © 2008, IGI Global**

Laws and Regulations Dealing with Information Security and Privacy:
An Investigative Study

John A. Cassini, Université d'Angers, France

B. Dawn Medlin, Appalachian State University, USA

Adriana Romaniello, Universidad Rey Juan Carlos, Spain

ABSTRACT

The Internet has dramatically transformed our lives in the past generation; and as our society has become dependent on information technology and more and more of our sensitive information is stored and transferred in electronic form, greater attention is being paid to privacy and security concerns. Governing bodies from states to national entities have passed laws and regulations that are designed to address and impact security and privacy practices. In this article we will examine the laws and regulations of the United States and the European Union (EU) in relationship to the issue of information security and privacy.

Keywords: *legislation; international law; information privacy; security*

INTRODUCTION

Administrators responsible for securing data and applications have two main goals. One is to prevent unauthorized access to information technology (IT) resources, such as a consumer's or patient's information. The other is to maintain IT services so that they are kept up-to-date.

To address the first goal, access controls are an obvious tool for preventing unauthorized access; but less obvious practices, such as auditing for unauthorized hardware, are also important. As an example, consider an unauthorized wireless access point in an office transmitting confidential consumer or patient information over an unencrypted Wi-Fi network. Anyone with a wireless network card could intercept the traffic. This highlights the fact that all the effort that went into defining, implementing, and managing access control policies could easily be circumvented.

The second goal of the administrator is the maintenance of IT services. This generally requires a multifaceted approach that includes firewalls and intrusion detection systems, as

well as antivirus services, scanning for vulnerabilities, and system configurations for controlling system security. Another important measure is to ensure that operating systems are appropriately patched. Both of these goals are important to protect information and for the network to function effectively. If guidelines, policies, and management recommendations are not followed, systems are vulnerable to security breaches that can range from simple nuisances, such as the implanting of spyware that slows the performance of desktops, to the crippling of networks through a distributed denial-of-service (DoS) attack that can effectively disable network services.

Of course, these in-house measures are necessary but in themselves insufficient to guarantee full security and protection in today's world of ever-expanding Internet use. As in every other aspect of our modern lives where communication and exchange occur between individuals, institutions, agencies, and businesses, the government has had to step in to regulate and legislate proper use and protection from abuse of the technologies that facilitate that communication.

To reach these aforementioned goals and repair breaches, systems administrators must be aware of and address current laws, directives, and regulations dealing with privacy and security issues. Certainly, the growth of the Internet as a file storage and transfer medium has forced society to reexamine the notions surrounding privacy and security.

This reexamination is especially necessary, as the use of the Web permeates our society, and the skills of those who use the Internet for criminal purposes also become more and more sophisticated. This in turn necessitates increasingly sophisticated and restrictive legislation and regulation in an attempt to maintain the clearly beneficial uses of the Internet, while keeping the forces of abuse and the temptation to violate privacy rights at bay.

To further complicate the issue, definitions of "privacy" protection differ depending on the country or the area of the world. In the United States protection of privacy is grounded in the protection of "liberty." In United States it is understood that privacy is ensured only when the government does not interfere. As a consequence of this conception of privacy as liberty, the legal framework for privacy in the United States is disjointed and piecemeal. The legal theory connecting the various protections of privacy is disjointed; several branches of law have developed, all growing from the seed of privacy protection but based on differing theories of what should be protected (De Vries, 2003).

In the European Union, however, the approaching to the question of privacy relies on the "dignity" of the individual. This legal framework responds to the concept of protection of privacy as protection of dignity which is different from the protection of liberty. Dignity is a social concept, whereas liberty is a political value. To protect dignity is to protect a certain social status, a certain image of one that society holds. Following Levin and Nicholson (2006), the concept of privacy as dignity explains much about Europeans´ aggressive position on private sector regulation as well as their relative lack of concern over government intrusion.

These two differing approaches to the concept of privacy explain the differences between United States and European Union in their regulation. While the European Union centrally supervises the private sector's use of personal data, the regulation of the private sector is minimal in the United States (Levin & Nicholson, 2005). It is beyond the scope of this article to deal fully with both systems.

For the purpose of our research we focus our attention on the security and privacy of information in the electronic communications sector. Therefore, it is the purpose of this article to provide a brief overview of the development of the Internet and to review certain major laws in the United States and the European Union that demonstrate the attempts to control security while protecting privacy. In particular, we will focus on the 2006 EU Directive which is significant because not only does it amend Directive 2002/58 EC (2007), but it also prioritizes