Chapter 2
Forty Years of Federal Legislation in the Area of Data Protection and Information Security

John Cassini
Université d'Angers, France

B. Dawn Medlin
Appalachian State University, USA

Adriana Romaniello
Universidad Rey Juan Carlos, Spain

ABSTRACT

Historically, the United States has attempted to address the issues of an individual's right to information privacy and security through legislative actions. More specifically, the execution of legislation that addresses information security and privacy has been implemented in particular areas such as health care, banking, and education as well as other industries. This chapter presents an overview of the laws that have addressed the growth of security and privacy threats that havegrown over the years.

INTRODUCTION

Founded in the 1950s, the Internet was initially designed to be a military communications network. Due in part to its popularity among scientists, it was later expanded to university campuses across the United States. Next came the introduction of the Internet to the public in the early 1990s, and since that time the Internet has grown at an exponential rate. This growth has certainly led to many benefits such as banking and bill paying online as well as electronic medical records. Unfortunately, as the number of people connecting to and using the Internet increases, so does the opportunity for fraudulent and malicious activities.

While the enormous popularity of the Internet was not foreseen, neither was the need for restrictive legislative action. Therefore, there was an

DOI: 10.4018/978-1-61692-000-5.ch002

initial period of legislative non-responsiveness as policy makers could not foresee the legal issues that might surround the use of the Internet. Even if the Internet would have had laws and restrictions in place during its fast-paced evolution, chances are the Internet would have never grown to the size and popularity it enjoys today (Wisebrod, 1995).

To better understand the order that is being imposed upon that initial chaos, we will address security and privacy issues from a chronological perspective, by presenting the major laws and regulations enacted by the United States government over the last 40 years. The provisions contained in these laws and regulations show how the topic of security and privacy of information has evolved over time as our society has fully adopted a continually evolving Internet as an integral part of its daily life and activities.

A chronological view of the evolution of information security and privacy laws and regulations can provide a rich observation of the relationship between technology and the law. It can also show how developments in technology bring about new uses and misuses of that technology and call forth more specific legal controls. The chronological approach can also provide insight as to how these laws have evolved over time as the United States society has evolved in its use of the Internet and other related technologies.

BACKGROUND

Technology plays an important role in providing current and up-to-date information for consumers and organizations as well as the instantaneous sharing of information between individuals using programs such as email or instant messaging. Most consumers would agree that technology can provide the accessibility of their information, and that fact alone is advantageous, but consumers are also becoming increasingly aware of the potential harmful impact of the misuse of these same technologies.

Certainly, Internet technologies have brought with them legal challenges that are often hard to define. Because we are a society governed by laws, information technology managers and systems administrators must be aware of and address current laws, directives and regulations dealing with cybercrime issues. In addition, the growth of the Internet as a file storage and transfer medium has forced society to reexamine the notions surrounding privacy and security issues.

As the worldwide economy continues to become more dependent upon information technologies, and as economies become more interdependent, it appears that security-based threats will continue to increase, with concomitant increases in costs to individuals, organizations, and society as a whole (Conca, Medlin, Dave, 2005). Researchers continue to look at the rise of professional cybercrime as a uniquely worrying phenomenon (Antonopoulos, 2009).

No matter the organizational type, one of the greatest problems faced by any company is the myriad of ways their IT structure and services can be diminished by malware or third-party attacks. The security-based threats and vulnerabilities that currently exist, such as Trojan Horses, spyware, and other types of malicious code, have the potential to damage consumers', as well as businesses', data or other assets. When organizations determine the asset risk, they must address the vulnerabilities that exist in order to protect themselves from loss of physical and tangible assets.

In order to address these aforementioned security threats, network or security administrators often find themselves in an endless cycle of applying patch after patch in an attempt to plug all the possible holes. While patches can take care of problems in software design, they cannot account for human error, lack of security knowledge, or the ever-growing threat from malware that can be continuously introduced, as employees increasingly use the Internet for both business and personal activities.

Related Content