Chapter 45
The Evolutionary Path of Legal Responses to Cybercrime Threats Over the Last Decade

Krassie Petrova
Auckland University of Technology, New Zealand

B. Dawn Medlin
Appalachian State University, USA

Adriana Romaniello
Universidad Rey Juan Carlos, Spain

ABSTRACT

Information and communication technologies have transformed our lives. In the United States, we have become more dependent on these technologies and more of our sensitive information is stored and transferred in electronic form, thus requiring greater attention to the privacy and security of that information. To protect an individual's information, laws and regulations that are designed to impact cybercrime activities have been enacted. From the study of American laws we can observe an evolutionary process in relation to computer crimes. In this chapter, the authors explore the growth of cybercrime threats that have grown over the last decade as well as their legislative responses.

INTRODUCTION

The growth of the Internet as a file storage and transfer medium has forced society to reexamine the notions surrounding cybercrime and more specifically the issues of security and privacy. Because we are a society governed by laws, in striving to reach the goal of stopping computer crimes and repairing breaches, current laws and regulations must address these crimes with a proactive stance.

The cyber law environment has not been fully defined by the court system in the U.S. Laws have been enacted, but until they are fully tested and explored by cases in court, the exact limits are somewhat unknown. This makes some aspects of the laws surrounding issues of computer crimes more challenging.

DOI: 10.4018/978-1-61520-847-0.ch045

Computer security though is no different from any other subject in our society. As our lives are affected by the threats of cybercrimes new laws must be enacted to enforce certain desired behaviors. The one substantial difference between this aspect of our society and others is that the speed of advancement in the information systems world driven by business, computer network connectivity, and the Internet only increases the opportunity for fraudulent behavior.

In this chapter, we will discuss current laws and regulations as applied to cybercrimes in the United States. This discussion includes laws related to such areas as health care, financial services and marketing that demonstrate the complexity of the issue of cybercrime and the legal system. Understanding the progression of these crimes as well as the associated laws may allow for individuals, organizations, as well as governmental agencies involved within the system to have a better understanding of how to protect and secure information. If we can learn from history, we may be less likely to repeat the same mistakes.

BACKGROUND

Cybercrime is a term that is quite difficult to define as it is described differently by even the experts within the information systems and criminal justice field of research. Some experts believe that cybercrime is nothing more than an ordinary crime such as larceny or trespassing that is committed using a computer, while other experts view cybercrime as a new type or a new category of crime, thus requiring new laws and regulations (Evans, Martin & Poatsy, 2009). Additionally, cybercrime has been defined as a subset of computer crime. Another definition of cybercrime includes networked services that can be disrupted or data that can be damaged or destroyed, rather than having data stolen or misused. This is referred to as "destructive cybercrime" (Cross, 2008, pg. 19).

In the 1980s and 1990s, cybercrime was mainly defined by the use of virus and worm attacks, that could exact some form of damage, yet the gains were generally negligible. Entering into and during the 21st century was the introduction of newer and more sophisticated forms of cybercrime such as malware, rootkits, and targeted attacks; criminals began to guide their attacks against individuals in order to obtain larger financial and informational gains. Cybercriminals though still commit crimes by introducing worms, viruses, and other malicious code into a system as well as mounting DoS attacks or vandalizing networked systems. Today, a more common activity of criminal crime is the use of computer actions that in some way deprives consumers of the use of the network and/or access to their information.

Another one of today's most common types of computer-based criminal activity is click fraud. Click fraud involves a piece of malware that defrauds the advertising revenue counter engine through fraudulent user clicks. For instance, sites like eBay, one of the leaders in the Internet auction space, and its companion PayPal, are frequent targets of fraud. Whether the fraud occurs through the fraudulent listing of items or fraudulent bidding, the results are the same – a crime has been or is being committed – that of fraudulent activities.

As the Internet has matured, more and more data is constantly being uploaded and stored online. Therefore, it should not be surprising that every type of data from personal information to financial figures is located on computers that are linked globally via the Internet. The linkage of information has had a profound and dramatic affect on cybercrime growth as individuals are able to coordinate their activities using not only a computer, but other individuals, in their quest to obtain financial gain.

Though the definitions of cybercrime may be slightly different in their focus, each of these definitions does include the need for legislation, either directly or indirectly. Therefore, to better understand the topic and surrounding legal is-