U.S. Information Security Law and Regulation

Michael J. Chapple
University of Notre Dame, USA

Charles R. Crowell
University of Notre Dame, USA

INTRODUCTION

The American legal system, along with many of its counterparts around the globe, is only beginning to grapple with the legal challenges of the knowledge age. The past decade has witnessed a multitude of new laws and regulations seeking to address these challenges and provide a common framework for the legal and technical professions. Those charged with information security responsibilities face a myriad of complex and often vague requirements. In this article, we establish a four-level taxonomy for information security laws and explore the major components of each level.

BACKGROUND

Mohamed Chawki, in a study of computer crime law, points out that the traditional definition of a computer crime as any crime that involves "the knowledge of computer technology for its perpetration, investigation, or prosecution" is far too broad for practical application (Chawki, 2005, p. 7). Virtually every crime involves computer technology at some point in the investigative process. For example, a common burglary should not be considered a computer crime merely because the booking officer entered data on the crime into a department information system. Similarly, the fact that the criminal looked up driving directions on the Internet should not make a bank robbery a computer crime.

We seek to clarify these issues by creating a general taxonomy of information security laws. Our taxonomy includes the following four levels:

- **Intellectual property laws** protect the rights of authors, inventors and creators of other intellectual works.
- **Computer-focused crime laws** define transgressions and applicable punishments for offenses where the use of a computer is intrinsic to the crime.
- **Computer-related crime laws** are those laws that involve the use of a computer but where the criminal activity is not defined by the use of a computer. This category also includes those laws that require the use of computers to assist in the investigation of a crime.
- **Industry-specific laws** do not apply to society as a whole but, rather, govern particular industries and are typically focused on protecting the confidentiality, integrity and/or availability of personal information.

It is also important to note that many information security crimes are prosecuted under traditional laws, rather than the specific laws presented in this taxonomy. Smith (2005) points out two examples of this: the charging of an individual with a felony offense for accessing an unprotected wireless network and a school district's charge of criminal trespass against 13 students who accessed laptops issued to them with an administrative password that was taped to the bottom of the machines.

In the remainder of this chapter, we seek to explore this taxonomy in further detail. While the taxonomy may be applied to any body of law, due to space constraints, this article limits the discussion to federal laws in the United States. A myriad of state and local laws, as well as the laws of other nations, may also be classified under this taxonomy.

INTELLECTUAL PROPERTY LAW

The legal principles protecting the rights of owners of creative works date back several centuries. As our society shifts from an industrial economy to a knowledge economy, these laws become increasingly important, as they protect the very essence of our economic engine. These intellectual property laws are critical to any information security program, as they provide the legal basis for protecting the intellectual property rights of individuals and organizations.

Copyrights

Copyrights protect any original work of authorship from unauthorized duplication or distribution. The Copyright Act defines eight categories that constitute covered works (Copyright Act, 1976). One of these categories, literary works, is broadly interpreted to include almost any written work. This category has traditionally been used to include computer software, web content and a variety of other works of direct interest to information security professionals.

Copyright protection is automatic upon the creation of a work. For works created after 1978, copyright protection lasts for 70 years after the death of the last surviving author.

Trademarks

Trademark law protects words, phrases and designs that identify the products or services of a firm. The essential characteristic of a trademark is that it must uniquely distinguish the trademark holder's goods or services from those of other providers. Therefore, trademarks may not be simply descriptive of the product or service but must contain the element of uniqueness. For example, it would not be possible to gain trademark protection on the term "blue automobile," while it may be possible to gain protection for the term "Blue Streak Automobiles".

Trademark protection is afforded by the Lanham Act (1946). The U.S. Patent and Trademark Office grants registrations with an initial duration of 10 years and the option to renew.

Patents

Patents protect inventions, processes, and designs. They grant the inventor substantial protection in the form of exclusive rights to the patented concept. To protect against the abuse of this privilege, the U.S. Patent and Trademark Office strictly governs the issuance of patents. The three requirements for patent protection are that the invention must be novel, useful, and nonobvious. Patents granted for inventions or processes are valid for 17 years while design patents are valid for 14 years (Patent Act, 1952).

Trade Secrets

The Economic Espionage Act of 1996 makes it illegal to steal, misappropriate, duplicate or knowingly receive or possess a trade secret without appropriate permission. Trade secrets include any information that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by the public" and are the subject of "reasonable measures to keep such information secret" (Economic Espionage Act, 1996).

When designing an information security program, it is essential to recognize that trade secrets are defined by the confidentiality protection afforded them. If an organization fails to take reasonable efforts to maintain the confidentiality of a trade secret, this protection is lost. This is a major departure from patent protection, which requires public disclosure of the invention. Public disclosure of a trade secret nullifies the protection afforded to that secret and effectively releases it into the public domain. Unlike patents, however, trade secrets enjoy indefinite protection under the law.

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (1998) instituted a number of significant changes in U.S. copyright law. In addition to procedural changes required to implement World Intellectual Property Organization (WIPO) treaties, DMCA makes several modifications to the law designed to accommodate the changing digital environment of the Internet. For example, DMCA offers a safe harbor provision for Internet service providers, absolving them of liability for the infringing acts of customers, provided that they have policies to terminate the accounts of repeat copyright offenders and do not interfere with the technical measures used by copyright holders to protect their works. If providers meet these requirements, they are protected from liability caused by transitory communications, system caching, information residing on systems or networks at the direction of users and information location tools (such as search engines).

COMPUTER-FOCUSED CRIME LAW

Computer-focused crime laws center upon the transgressions and associated punishments when the use of a computer is intrinsic to the crime. When drafting computer-focused crime laws, legislators have the specific intent of outlawing the use of a computer to commit a crime. This category is distinct from the next category, computer-related crime laws, crimes in which the perpetrator may utilize a computer as a support tool. For example, a law prohibiting the use of a computer to eavesdrop on the electronic mail of an individual is a computer-focused crime law. It is the act of using the computer to eavesdrop that is the essential nature of the crime.

Computer Fraud and Abuse Act

Congress originally passed the Computer Fraud and Abuse Act of 2001 in 1986 and later amended it in 1994, 1996, and 2001 to reflect the rapidly changing digital environment. Originally intended to protect data contained on the computers of government agencies and financial institutions, later amendments expanded the scope to include any system involved in interstate commerce (Burke, 2001). Offenses under the Computer Fraud and Abuse Act include gaining unauthorized access to a computer.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA) of 1986 protects the rights of individuals who become the subject of electronic surveillance by government agencies or other third parties. It includes two separate components: the Wiretap Act and the Stored Communications Act (SCA).