Cyberlaw Statutes in the USA

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Relatively few information security practitioners have a grasp of the legal environment in which they work. Exceptions include CISSPs, who must demonstrate and maintain their knowledge of laws pertaining to computer crime, privacy, and other information security matters. This article introduces some of the most important laws governing cyberspace crime in the United States.

The most advanced set of laws criminalizing particular unlawful behavior involving computers and networks have been legislated in the United States. The *Computer Fraud and Abuse Act of 1986* (18 USC §1030) focuses primarily on protecting “government-interest” computers, including federal, state, county and municipal systems; financial and medical institutions; and computers used by contractors supplying such institutions. Specifically, the Act prohibits the use of “a program, information, code or command” with intent to damage, cause damage to, or deny access to a computer system or network. In addition, the Act specifically prohibits even unintentional damage if the perpetrator demonstrates reckless disregard of the risks of causing such damage.

Another law governing interstate electronic communications has been used in prosecutions of computer crimes: 18 USC §1343, dealing with wire fraud. Wire fraud requires the following elements: (a) a scheme to defraud by means of false pretenses; (b) knowing and willful participation with intent to defraud; (c) the use of interstate wire communications in furtherance of the scheme.

The Electronic Communications Privacy Act of 1986 (18 USC §1367 and others), generally known as the ECPA, assigns fines and prison sentences for anyone convicted of unauthorized interception and disclosure of electronic communications such as phone calls through land lines or mobile systems and e-mail. In addition, the ECPA specifically prohibits making use of an unlawfully overheard electronic communication if the interceptor knows that the message was unlawfully obtained. On the other hand, providers of electronic messaging systems, including employers, are permitted to intercept messages on their own systems in the course of their normal operations; naturally, they are authorized to transmit messages to other communications providers as part of the normal course of transmission to the ultimate recipient. The ECPA also prohibits access to stored messages, not just those in transit.

United States law also criminalizes the use of interstate communications for the transmission of threats, in kidnappings, and in extortion (18 USC §2518). Another form of prohibited speech is everything associated with child pornography: making, sending, publishing or storing images of children engaged in sexually explicit conduct (18 USC §2251).

The Communications Decency Act of 1996 (47 USC §223) was a highly controversial statute prohibiting anyone using interstate or communications from transmitting obscene or indecent materials when they know that the recipient is under 18 years of age – regardless of who initiated the communications. In June 1997, in a stinging rebuke to proponents of censorship, the United States Supreme Court issued its ruling on the Communications Decency Act, finding that it violated First Amendment protection of free speech. The unanimous opinion stated that the
effort to protect children from sexually explicit material went too far because it also would keep such material from adults who have a right to see it.

In addition to federal laws, the United States has a tapestry of state laws applying to computer crimes. States differ widely in the availability of computer-crime laws and in their definitions and penalties.

* * *

For further reading:


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.