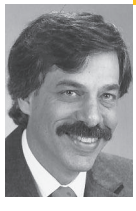
DANIEL L. APPELMAN

primer on cybercrime laws



Dan Appelman is a partner in the law firm of Heller Ehrman LLP (www.hewm.com) and is the lawyer for the USENIX Association. He practices technology law in Menlo Park, California. Dan writes and speaks frequently about legal issues important to computer programmers, system administrators, and technology companies generally.

dan@hewm.com

AS CYBERCRIME PROLIFERATES AND cybercriminals become ever more creative, it is important for those who maintain the integrity and security of computer systems and data networks to understand the key sources of cybercrime law that protect those systems and networks from abuse. This article describes the sources of cybercrime law in the United States.

Cybercrime laws fit roughly into three categories: (1) laws concerning crimes against computer systems, (2) laws concerning crimes against communications systems, and (3) laws concerning crimes facilitated by computers and the Internet.

Laws Addressing Crimes Against Computer Systems

In the United States, the principal federal criminal law protecting computer systems is the Computer Fraud and Abuse Act (CFAA) [1]. Passed by Congress in 1984 and amended several times since [2], the law makes it a crime to:

- access a computer without authorization to obtain classified information pertaining to national defense or foreign relations with reason to believe that such information so obtained could be used to the injury of the United States or to the advantage of any foreign nation; and to willfully retain that information or to transmit it to any person not entitled to receive it;
- intentionally access a computer without authorization to obtain information (1) contained in a financial record of a financial institution or credit card company or contained in a file of a consumer reporting agency on a consumer, (2) from any department or agency of the United States, or (3) from any "protected computer" [3] if the conduct involves interstate or foreign communication;
- intentionally access without authorization (1) any "nonpublic" computer of the United States government if the computer is exclusively reserved for the use of the government, or (2) any computer used by or for the government (even nonexclusively) if such access affects the government's use or purpose;
- knowingly and with intent to defraud, access a protected computer without authorization and, by means of such conduct, further the intended fraud and obtain anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of

REFERENCES

[1] 18 USC § 1030 et seq., http://www.usdoj.gov/criminal/cybercrime/1030_new.html.

[2] Most recently amended in portions of the USA Patriot Act of 2001.

[3] The term "protected computer" means a computer (1) exclusively for the use of a financial institution or the United States government or (2) which is used in interstate or foreign commerce or communication. A computer can be located outside the United States and still qualify as "protected" for purposes of the CFAA.

[4] 18 U.S.C. § 2510 et seq., http://www.usdoj.gov/criminal/cybercrime/wiretap2510_2522.htm.

[5] See, e.g., Reno v. ACLU, 521 US 844 (1997).

[6] The exception is trade secrecy, where state laws, not federal, govern.

such use is not more than $5,000 in any one-year period;

- knowingly cause transmission of a program, information, code, or command and as a result intentionally cause damage to a protected computer or intentionally access a protected computer and cause damage to it, if such damage includes (1) a loss by one or more persons aggregating to at least $5,000 in any one year, (2) the alteration of data concerning the medical examination, diagnosis, treatment, or care of any person, (3) physical injury to any person, (4) any threat to public health or safety, or (5) damage that affects a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
- knowingly and with intent to defraud, traffic in any password or similar information through which a computer may be accessed without authorization, if (1) such trafficking affects interstate or foreign commerce, or (2) such computer is used by or for the government of the United States;
- transmit in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer with intent to extort from any person any money or other thing of value.

Actions in violation of the CFAA are criminal offenses punishable by fines and imprisonment of up to 20 years.

Many states have their own laws making it illegal to access or cause damage to computer systems. Illegal activities under state law often include: (1) unauthorized access to a computer system or network; (2) modifying, damaging, or misappropriating programs or data; (3) introducing a virus or damaging code into a computer system; (4) using a computer to defraud; (5) interfering with someone else's computer access or use; (6) using encryption to facilitate a crime; and (7) falsifying email header information. The laws addressing crimes against computer systems vary greatly from state to state. A survey of those laws is beyond the scope of this article.

Laws Addressing Crimes Against Communications Systems

The United States has long had laws making it a crime to intercept and capture wire-line and wireless communications. The Electronic Communications Privacy Act of 1986 (ECPA) [4] amended various parts of the federal criminal code to make existing law more relevant to communications facilitated by computers and data networks.

Section 2511 of the ECPA prohibits the interception, disclosure, and use of certain wire, oral, and electronic communications; and Section 2510 defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."

Section 2511 also exempts certain "providers of electronic communication services" (e.g., telephone companies and Internet service providers) from liability under the Act if their interception, disclosure, or use of communications flowing through or stored on their systems occurs while the providers are engaged in any activity which is a necessary incident to the rendition of their services or to the protection of their rights or property. The ECPA also exempts those providers from liability for disclosing electronic communications to third parties who have been authorized by law to receive them (e.g., the Recording Industry Association of America in its efforts to learn the identities of those who make available and/or download music from various Internet sites).

Section 2512 prohibits the manufacture, distribution, possession, and advertising of certain wire and electronic intercepting devices. Other sections of the ECPA give law enforcement authorities permission to confiscate such devices and limit the use of intercepted communications as evidence in criminal prosecutions.

Laws Addressing Crimes Facilitated by Computers and the Internet

In addition to the laws protecting the integrity and security of computer and communications systems themselves, many federal and state laws and regulations prohibit the use of those systems to commit other offenses. The types of crimes and other illegal activities that can be facilitated by computers and communications systems are too numerous to set forth exhaustively here, but three of the major categories are (1) fraud, (2) pornography and obscenity, and (3) infringement of intellectual property rights.

FRAUD

Fraud is increasingly committed with the assistance of computers and the Internet. Often, fraud is prosecuted by federal and state authorities under generic statutes that have little or no reference to the computer and communications systems that are used. The interstate nature of the Internet can help to "bootstrap" these activities to the status of federal crimes where otherwise only the state law enforcement agencies would

have jurisdiction. But states are increasingly enacting their own laws that have as their key elements the use of computers and data communications systems in commission of the unlawful activities.

Within the category of fraudulent activities, identity theft is of growing concern. Congress has been slow to enact federal laws making identity theft a crime. As a result, a number of states have passed laws requiring the owners of electronic databases containing personal information about consumers both to meet minimal security standards and to inform those consumers when that information has been compromised.

On the federal level, fraud is prosecuted mainly by the Federal Trade Commission under various consumer protection laws. However, its budget for such activities is limited and it lacks the resources to investigate and then take action on most of the complaints it receives. Thus far, most of the action has therefore been on the state level, with considerable variance among the states with respect to defining the crimes and penalties. Recently, a number of bills have been introduced at the federal level that would, if enacted into law, make for a more uniform application of the law to fraudulent cyber-activities.

PORNOGRAPHY AND OBSCENITY

The regulation of the display and dissemination of pornographic and obscene material has historically been left to the states, with a few Supreme Court cases providing guidance where First Amendment issues become relevant. Congress tried to pass several laws making it a crime to display certain kinds of sexually oriented material on the Internet, but the Supreme Court subsequently rejected most of the prohibitions because of their chilling effect on free speech [5]. As a result, most computer- and Internet-specific laws limiting speech (and the display of pornographic and obscene materials in particular) have been struck down when challenged.

INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS

In the United States, intellectual property rights are largely protected by federal laws, leaving little room for independent state legislative activities [6]. The proliferation of personal computers and the expansion of the Internet have made it easy to duplicate and distribute materials protected by copyright law without the permission of the owners of those materials.

In 1998, Congress passed the Digital Millennium Copyright Act (DMCA), which, among other things, made it a crime to circumvent anti-piracy measures built into computer software and other digital materials and also to manufacture or sell devices that can be used to facilitate such circumvention. The DMCA has survived legal challenges and has been used by several organizations representing copyright owners to prosecute infringers.

Summary and Conclusion

In the United States, laws addressing cybercrime have been enacted both by Congress and by a number of state legislatures. The federal laws are fewer and in general quite narrowly drafted to survive constitutional and other challenges. States have passed laws where Congress has not yet acted and also where federal regulation has been ineffective. As a result, many types of cybercrime are addressed only by state laws, and those laws vary significantly from state to state.

In many respects, state legislation seems to be a particularly inefficient and inappropriate way to address cybercrime, given the interstate or, often, global nature of those activities. Inconsistent state definitions of what constitutes criminal activity prevent those with lawful intentions from relying on clear standards. And state law authorities find it impossible to enforce their laws against those who operate outside their jurisdictions.

States sometimes address the problem of inconsistent standards by adopting model laws offered by such organizations as the National Conference of Commissioners on Uniform State Laws. For example, most states have adopted versions of the Uniform Trade Secrets Act and the Uniform Commercial Code. As a result, the laws on trade secrecy and on commercial practices are remarkably similar from state to state. Proposals for uniform state cybercrime laws have been suggested but none have yet been adopted.

However, the adoption of uniform state cybercrime laws would not provide a satisfactory approach to dealing with cybercrime, because of the need for national and perhaps global standards and enforcement. A system of international laws on cybercrime is also unrealistic given the high priority most countries place on national sovereignty. The European Union serves as an example of how some countries have agreed to give up a certain measure of sovereignty for the benefit of harmonized regional laws. Until that model takes hold elsewhere, the most we can anticipate is increased federal legislative and regulatory activity that would preempt inconsistent state laws and provide a measure of predictability in the treatment of cybercrime in this country.