



Internet Crime

©2009 eNotes.com, Inc. or its Licensors. Please see [copyright information](#) at the end of this document.

- [Background](#)
- [Fraud](#)
- [Unauthorized Computer Access](#)
- [Damaging Communications Lines, Stations, or Systems](#)
- [Interception and Disclosure of wire, Oral, or Electronic Communications](#)
- [Terrorism](#)
- [Unlawful Access to Stored Communications](#)
- [Pornography and Sexual Predators](#)
- [Copyright Violations](#)
- [State Laws and Policing](#)
- [Additional Resources](#)
- [Organizations](#)

Background

Internet crime is among the newest and most constantly evolving areas of American law. Although the Internet itself is more than three decades old, greater public usage began in the late 1980s with widespread [ADOPTION](#) only following in the 1990s. During that decade the Net was transformed from its modest military and academic roots into a global economic tool, used daily by over 100 million Americans and generating upwards of \$100 billion in domestic revenue annually. But as many aspects of business, social, political, and cultural life moved online, so did crime, creating new challenges for lawmakers and law enforcement.

Crime on the Net takes both old and new forms. The medium has facilitated such traditional offenses as [FRAUD](#) and child [PORNOGRAPHY](#). But it has also given rise to unique technological crimes, such as electronic intrusion in the form of hacking and computer viruses. High-speed Internet accounts helped fuel a proliferation of [COPYRIGHT INFRINGEMENT](#) in software, music, and movie [PIRACY](#). National security is also threatened by the Internet's potential usefulness for [TERRORISM](#). Taken together, these crimes have earned a new name: when FBI Director Louis J. Freeh addressed the U. S. Senate in 2000, he used the widely-accepted term "cybercrime."

Lawmakers have scrambled to keep up with cyber-crime. The skyrocketing growth of Internet usage and the rapid advance of technology quickly revealed the inadequacy of existing laws, particularly those drafted to fight [COMPUTER CRIME](#) in the mid-1980s. In the 1990s, headlines frequently announced high-profile cyber crimes such as the estimated \$80 million in damages caused by the nationwide outbreak of the computer virus Melissa in 1999, unauthorized intrusion into military computer systems, and brazen hacker attacks that ranged from denying service to major [CORPORATE](#) websites to defacing U. S. government websites of the CIA, FBI, and others. Simultaneously, the computer software industry announced massive losses due to piracy, \$12 billion in 1999 alone, according to the Washington-based Business Software Association (BSA), the leading U.S. software industry watchdog. Regarding these concerns, Congress acted repeatedly. Its legislative response ranges from provisions governing hacking, viruses, and denial of service attacks to fraud, [OBSCENITY](#), copyright infringement, and terrorism.

Encyclopedia of Everyday Law: Internet Crime

- The COUNTERFEIT Access Device and Computer Fraud and Abuse Act of 1984 launched federal cybercrime law. The law safeguarded classified government information as well as certain financial information stored digitally, while also creating offenses for malicious damage of computer systems and trafficking in stolen computer passwords. It was superseded by the Computer Fraud and Abuse Act of 1986, which was amended significantly in 1994, 1996, and 2001, and remains the backbone of federal Internet law.
- The Electronic Communications Privacy Act of 1986 was passed to prevent the unauthorized interception of digital communications and later amended to specifically bar unauthorized reading of e-mail by third parties, network operators, and Internet access providers.
- The National Information Infrastructure Protection Act of 1996 expanded the Computer Fraud and Abuse Act. Amendments covered the confidentiality, integrity, and availability of computer networks, essentially broadening the definition of computer hacking punishable under federal law.
- The No-Electronic Theft Act (NET Act) of 1997 tightened restrictions on the reproduction and dissemination of copyrighted intellectual property like software, music, and movies, while the Digital Millennium Copyright Act (DMCA) of 1998 prohibited the circumvention of copyright protection systems.
- The Communications Decency Act (CDA) of 1996 criminalized the dissemination of obscene or indecent material to children over computer networks. It was ruled unconstitutional under the First Amendment in 1997.
The Child Online Protection Act (COPA) of 1998 modified the scope of the CDA by criminalizing the use of the World Wide Web to sell material harmful to minors. It, too, was ruled unconstitutional in a case that has since been granted review by the Supreme Court.
- The Protection of Children from Sexual Predators Act of 1998 included Internet-specific provisions for reporting child pornography to authorities and prohibiting federal prisoners from unsupervised Internet usage.
- The Patriot Act of 2001 was passed in response to terrorist attacks upon the United States. Modifying the Computer Fraud and Abuse Act, it provides new investigative powers to the U. S. attorney general to order monitoring of Internet communication and usage for the purpose of protecting national security.

Fraud

Fraud is the broadest category of cybercrime. Fraud includes many types of criminal activity, ranging from credit card abuse, wire fraud, and business fraud to misrepresentation and the failure to deliver purchases. The Federal Trade Commission monitors and regulates Internet commerce, and it maintains advice for avoiding fraud at its website: <http://www.ftc.gov/bcp/menu-internet.htm>. The Federal Bureau of Investigation investigates and prosecutes cybercrimes. In partnership with several federal agencies, the FBI maintains the Internet Fraud Complaint Center online for accepting complaints at <http://www1.ifccfbi.gov/index.asp>.

Traditional [CONSUMER PROTECTION](#) laws apply to fraud on the Internet, but federal law also contains specific Internet-related laws as well. First among these is fraud involving access devices. Federal law defines access devices as cards, codes, account numbers, serial numbers, and so forth that are used to obtain money, goods, and services or to initiate a transfer of funds. A typical example is the [FRAUDULENT](#) use of another person's credit card over the Internet.

The law targets several forms of fraud regarding the use of access devices:

- Producing, using, or trafficking in access devices
- Obtaining anything of value aggregating \$1,000 or more during a one-year period

- Possessing fifteen or more counterfeit or unauthorized access devices
- Possessing or controlling [COUNTERFEITING](#) access device equipment
- Effecting transactions with access devices issued to another person
- Offering to sell access devices or information on how to obtain them
- Possessing equipment modified to obtain unauthorized use of telecommunications services
- Possessing "scanning receivers" capable of intercepting wire or electronic communication
- Possessing hardware or software that modifies telecommunications identifying information in order to obtain unauthorized telecommunications service
- Unauthorized charges to credit cards

Penalties for violations range from fines to [IMPRISONMENT](#) from between five to 10 years per offense.

Unauthorized Computer Access

Types of Unauthorized Access

Popularly known as hacking, unauthorized computer access is a crime punishable under the Computer Fraud and Abuse Act (as codified in 28 U.S.C. § 1029). The law begins by defining hacking in two ways:

- Unauthorized access to computer systems
- Access that exceeds a person's authorized limits

The prohibition thus covers trespassers who have no right at all to use a given computer, as well as those who are allowed to use a given computer but manage to access parts of the system that are off limits.

National Security

The Computer Fraud and Abuse Act creates a separate offense of unauthorized or exceeded authorization in access for purposes that are damaging to national security. These crimes include obtaining state secrets protected by [STATUTE](#) or Executive order, along with military data or any information governed by the Atomic Energy Act of 1954, when such information could be used to injure the nation or to provide an advantage to a foreign nation. Minimum penalties may include fines, imprisonment for up to ten years, or both.

Illegally Obtaining Information

Federal law broadly prohibits hacking in order to gain information. It criminalizes obtaining three categories of information from different types of computer systems:

- Financial data, including records of financial institutions, credit card companies, and credit bureaus
- Information from any department or agency of the United States
- Information from any computer used in interstate or foreign communication

These are known in the Computer Fraud and Abuse Act as "protected" computer systems. The last category—computers used in interstate or foreign communication - essentially covers most computers connected to the Internet. The law does not go into detail on the types of information it intends to protect; instead, the intent is to prohibit unauthorized access to any information on protected systems. Minimum penalties may include fines, imprisonment for up to one year, or both.

Affecting U.S. Government Computers

The law forbids any unauthorized access of computers belonging to, or used by, a department or agency of the U. S. Government if the access merely "affects" their usage. As with the prohibition on gaining unauthorized information, the law is generally written in broad language to encompass the widest range of possible offenses. Minimum penalties may include fines, imprisonment for up to one year, or both.

Intent to Defraud

A separate offense occurs when a person gains unauthorized access with the intent to [DEFRAUD](#). The law is violated if anything of value is obtained. Minimum penalties may include fines, imprisonment for up to five years, or both.

Damaging Computers

Damage is defined as any impairment to the integrity or availability of data in any of four ways:

- The damage causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals
- The damage modifies or impairs, or potentially modifies or impairs, medical diagnosis, treatment, or care of one or more individuals
- The damage causes physical injury to a person
- The damage threatens public health or safety
- Three grades of damage to computer systems are defined. In increasing degree of severity, these are:
 - Damage
 - Reckless damage
 - Intentional damage

Damage is distinguished by criminal intent. Mere damage involves all forms of injury to data or equipment that were not intended yet still occurred. Reckless damage involves [NEGLIGENCE](#), the result of the criminal's carelessness. The third category, intentional damage, involves knowingly transmitting "a program, information, code, or command" that leads to damage. Examples of intentional damage include maliciously deleting files on a computer or releasing a computer virus or worm.

Convictions on any of the offenses can lead to fines, imprisonment, or both, with the prison sentences scaling upwards depending upon intent. Damage carries a [PENALTY](#) of one year of imprisonment. Reckless damage carries a penalty of up to five years imprisonment. Intentional damage is a [FELONY](#) and carries a penalty of up to five years.

Password Trafficking

Typically, passwords for computer access or online accounts are restricted to individuals. Since computer hackers often need to obtain them in order to enter systems without being detected, the law targets the illegal acquisition, sharing, or dealing in passwords. Two conditions trigger an offense:

- The trafficking must affect interstate or foreign commerce
- The computer is used by or for the U. S. Government

Minimum penalties may include fines, imprisonment for up to one year, or both.

Extortion

EXTORTION occurs when a person communicates a threat to damage a protected computer system with the goal of obtaining some reward, such as money. This element of the law addresses a widely publicized trend in the 1990s involving hackers who sought to profit from their ability to infiltrate the security of computer systems.

Unauthorized access with intentional extortion is an offense when committed upon any of the following:

- Person
- Firm
- Association
- Educational Institution
- Financial Institution
- Government entity
- Other legal entity

Minimum penalties may include fines, imprisonment for up to five years, or both.

Additional Penalties and Legal Recourse

The Computer Fraud and Abuse Act prescribes penalties for either attempting or actually committing its offenses. The minimum penalties for each offense are only available to first-time offenders who are not convicted in conjunction with other offenses under the law. For multiple and repeat offenses, the law doubles the prescribed imprisonment time.

Besides these criminal penalties, the law specifically provides for civil lawsuits. Thus anyone who suffers damage or loss through a violation of the Computer Fraud and Abuse Act can bring suit against the violator and seek [COMPENSATORY DAMAGES](#), court orders to end specific behavior, or other forms of relief. Such lawsuits must be brought within two years of the date of the complaint or the date of the [DISCOVERY](#) of the damage.

Damaging Communications Lines, Stations, or Systems

In addition to the damage provisions under the Computer Fraud and Abuse Act, broad protections to the nation's communication infrastructure are found in Federal law at 18 U.S.C. § 1362. The law criminalizes damaging any of the communications systems operated or controlled by the United States. These crimes include maliciously obstructing, hindering, or delaying the transmission of any communication. Penalties may include fines, imprisonment for up to ten years, or both.

Interception and Disclosure of wire, Oral, or Electronic Communications

Federal law protects communication over the Internet in much the same way it protects communication by the more traditional means of telephone and mail. Just as it has long been a federal offense to intercept another person's telephone calls or mail, it is illegal to intercept or disclose communications that occur over the Internet as e-mail, voice mail, Internet-based telephone calls, or any other private Internet-based communication.

Encyclopedia of Everyday Law: Internet Crime

Under 18 U.S.C. § 2511, federal law specifically protects individuals from eavesdropping and companies from industrial [ESPIONAGE](#). All third parties are prohibited from unauthorized interception or disclosure of private communications, except under certain exceptions. Exceptions to the prohibition cover employees of the Federal Communications Commission (FCC), law enforcement personnel, and the employees of Internet service providers. FCC employees may intercept communications in the course of monitoring responsibilities for enforcement of federal communications law. Generally, law enforcement personnel require court approval in order to intercept private communications; however, in certain cases involving national security, this is not required. Employees of Internet service providers are banned from intercepting private communications except in the normal course of their employment under certain exceptions:

- The interception is necessary incident to the rendition of his or her service or to the protection of the rights or property of the Internet provider
- Observing or random monitoring is only permissible for mechanical or service quality control checks
- The service has been ordered by law enforcement officials to intercept communications in the course of a criminal investigation

Penalties may include fines, imprisonment from one to five years, or both.

Terrorism

In response to terrorist attacks upon the United States on September 11, 2001, Congress passed the Patriot Act of 2001. This law provides several new powers to the U.S. attorney general to combat terrorism. Several provisions relate to cybercrime and electronic [EVIDENCE](#):

- Expanded authority for ordering wiretapping in a wider range of criminal investigations
- Relaxed restrictions for obtaining access to voice-mail and stored voice communications
- Expanded scope of data that can be subpoenaed, such as Internet access logs and other digital records of Internet usage
- Expanded authority for obtaining access to cable Internet records previously kept private by cable TV laws
- Provided grounds for Internet service providers to make voluntary emergency disclosures to law enforcement about customer records in emergencies involving immediate risk of death or serious physical injury to any person
- Removes geographical restrictions on tracing Internet and other electronic communication
- Expands authority to monitor actions of computer trespassers
- Permits federal courts to issue nationwide search warrants for e-mail
- Raises certain penalties for computer hackers to prevent and deter "cyberterrorism"
- Creates a new offense for damaging computers used for national security and criminal justice

Because of concerns about civil liberties, several of the new powers are temporary. Subject to so-called sunset provisions, they expire on December 31, 2005 unless renewed by Congress. Lawmakers built in these limitations in recognition of the potential for abuse of such powers, which they wished to limit to usage in combating the extraordinary dangers presented by the war on terrorism.

Unlawful Access to Stored Communications

Besides criminalized illegal interception of communication as it occurs, federal law prohibits unauthorized access to stored communications. Under 18 U.S.C. § 2701, it is illegal to intentionally gain access or exceed

authorized access to a facility that provides an electronic communication service, such as an Internet provider that handles e-mail. The law spells out two main offenses:

- Accessing the service without authorization or exceeding authorization
- Obtaining, altering, or preventing proper access to the service's stored communications

Minimum penalties include fines and prison sentences of six months. However, if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, prison sentences may range from one to two years.

Pornography and Sexual Predators

Federal law regarding pornography on the Internet remained tied up in the courts in 2001. During the previous decade, Congress twice enacted laws aimed at protecting children from exposure to pornography. The Communications Decency Act of 1996 broadly criminalized the dissemination of obscene or indecent material to minors over computer networks but was ruled unconstitutional the following year in *Reno v. ACLU*. In response, Congress modified the law, enacting the Child Online Protection Act (COPA) of 1998. COPA narrowed the scope of the previous law by criminalizing the act of selling material harmful to minors over the World Wide Web. Following a ruling that it was also unconstitutional, the case was on appeal to the Supreme Court with a decision expected in 2002.

However, while pornography remains widely available on the Internet, child pornography is treated severely under the law. Both federal and state law enforcement agencies routinely target child pornography online, and both U. S. Customs and the FBI maintain programs that encourage citizen reporting of criminal images of minors found on websites.

Specific Internet offenses are targeted in portions of the Protection of Children From Sexual Predators Act of 1998:

- Provides for the prosecution of individuals for the production of child pornography if the materials have been mailed, shipped, or transported in interstate or foreign commerce, including by computer
- Requires Internet service providers to report evidence of child pornography offenses to law enforcement agencies
- Prohibits Federal prisoners from being allowed Internet access without supervision by a government official, and urges that state prisons adopt the same policy
- Directs the attorney general to request that the National Academy of Science study technological approaches to the problem of the availability of pornographic material to children on the Internet

Copyright Violations

The problem of piracy — unauthorized storage, copying, or dissemination of copyrighted material such as computer software, music, movies and books — burgeoned along with the growth of the Internet. Existing federal copyright law makes it a crime to duplicate, store, or disseminate copyrighted materials for profit. But under the No Electronic Theft Act of 1997, it is also illegal merely to reproduce or distribute copyrighted works even without the defendant's having a commercial purpose or private financial gain. This aspect of the law targets the popular free trade of copyrighted material on the Internet.

Encyclopedia of Everyday Law: Internet Crime

Federal copyright law provides for both criminal and [CIVIL ACTION](#) against offenders. Criminal penalties may include fines, jail sentences up to three years, or both. Civil penalties can reach as high as \$150,000 per violation.

The Digital Millennium Copyright Act (DMCA) of 1998 marked the first significant revision of federal copyright law in a generation. Among its chief reforms, the law made it a criminal offense to bypass or defeat security provisions built into products by manufacturers to prevent copying. The applicability of that aspect of the law to the Internet was shown in *Universal City v. Reimerdes* (2001). In that high-profile case, a federal appeals court upheld a lower court verdict that a hacker website violated the DMCA by publishing information about defeating the anti-copying protection software built into movie DVDs.

State Laws and Policing

Most states have enacted Internet laws. Generally, these laws have evolved alongside and therefore mirror federal law. Most state Internet laws criminalize fraudulent use of computer systems for hacking, damage to computer systems, and unauthorized interception of communication. Several laws have enacted statutes that extend their existing laws on traditional crimes to the Internet, such as a 1995 Connecticut state law that targets online [STALKING](#): the law creates criminal liability for sending messages with intent to harass, annoy, or alarm another person. And while Congress in 2000 and 2001 often debated the issue, most states have enacted their own laws to ban online gambling.

More than a dozen states have passed laws targeting online pornography and sexual predators. Generally, these laws have sought to protect minors from access to porn or other material deemed harmful, such as California's 1997 law, or they have extended state child pornography laws to cover Internet images, as Kansas and Georgia both did as early as 1995. But as with federal legislation in this area, not all state laws have survived legal challenges. In 1997, a federal court overturned New York State's anti-pornography law in *ALA v. Pataki*, ruling that its ban on sending "indecent" materials to minors over the Internet was an unconstitutional regulation of commerce. Georgia was also prohibited in 1997 from enforcing a statute that made it a criminal offense to communicate anonymously over the Internet in an attempt to protect children from sexual predators; the law was held unconstitutionally vague and overbroad in *ACLU v. Miller*.

In the twenty-first century, states are also adopting proactive law enforcement policies. Examples include Washington State, which in 2000 launched a combined federal-state program called the Computer Law Enforcement of Washington (CLEW) initiative. Under CLEW, local, state and federal law enforcement agencies share information, maintain a high-tech crime strike force, and publish tips online to help fight fraud and other crime. Several states, such as New Jersey, established special cybercrime units in order to investigate crimes from industrial espionage to drug trafficking. Because of the cross-jurisdictional nature of much Internet crime, state attorneys general have also pursued innovative information-sharing programs. Legal observers expect to see further law enforcement cooperation among states.

Additional Resources

A Parent's Guide to Internet Safety. FBI, 2001. Available at: <http://www.fbi.gov/publications/pguide/pguide.htm>.

Computer Crime and Intellectual Property Section (CCIPS). Criminal Division of the U. S. Department of Justice, 2001. Available at: <http://www.cybercrime.gov>.

Encyclopedia of Everyday Law: Internet Crime

Consumer Protection: E-Commerce and the Internet. Federal Trade Commission, 2001. Available at: <http://www.ftc.gov/bcp/menu-internet.htm>.

Cybercrime. Statement by Louis J. Freeh, Director of Federal Bureau of Investigation, in Senate testimony, February 16, 2000. Available at: <http://www.fbi.gov/congress/congress00/cyber021600.htm>.

Internet Fraud Preventive Measures. FBI Internet Fraud Complaint Center, 2001. Available at: <http://www1.ifccfbi.gov/strategy/fraudtips.asp>.

Software Piracy and the Law. Business Software Alliance, 2001. Available at: http://www.bsa.org/usa/freetools/consumers/swandlaw_c.phtml.

U. S. Code, Title 18, Section 1029: Fraud and Related Activity in Connection with Access Devices. U.S. Congress. Available at: <http://www.usdoj.gov/criminal/cybercrime/usc1029.htm>.

U. S. Code, Title 18, Section 1030: Fraud and Related Activity in Connection with Computers. Available at: http://www.usdoj.gov/criminal/cybercrime/1030_new.html.

U. S. Code, Title 18, Section 1362: Communication Lines, Stations, or Systems. Available at: <http://www.usdoj.gov/criminal/cybercrime/usc1362.htm>.

U. S. Code, Title 18, Section 2511: Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. Available at: <http://www.usdoj.gov/criminal/cybercrime/usc2511.htm>.

U. S. Code, Title 18, Section 2701: Unlawful Access to Stored Communications. Available at: <http://www.usdoj.gov/criminal/cybercrime/usc2701.htm>.

U. S. Code, Title 18, Section 2702: Disclosure of Contents. Available at: <http://www.usdoj.gov/criminal/cybercrime/usc2702.htm>.

West Encyclopedia of American Law. West Group, 1998.

Organizations

Business Software Alliance (BSA)

1150 18th St. NW, Suite 700
Washington, DC 20036 USA
Phone: (888) 667-4722
URL: <http://www.bsa.org>
Primary Contact: Robert Holleyman, President

Federal Bureau of Investigation

J. Edgar Hoover Building, 935 Pennsylvania
Avenue, NW
Washington, DC 20535-0001 USA
Phone: (202) 324-3000
URL: <http://www.fbi.gov>

Encyclopedia of Everyday Law: Internet Crime

Primary Contact: Robert S. Mueller III, Director

Federal Trade Commission

CRC-240

Washington, DC 20580 USA

Phone: (877) 382-4357

URL: <http://www.fbi.gov>

Primary Contact: Timothy J. Muris, Chairman

National Infrastructure Protection Center

J. Edgar Hoover Building, 935 Pennsylvania
Avenue, NW

Washington, DC 20535-0001 USA

Phone: (888) 585-9078

Fax: (202) 323-2079

URL: <http://www.nipc.gov>

Primary Contact: Ron Dick, Director

Copyright Notice

©2009 eNotes.com, Inc.

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, Web distribution or information storage retrieval systems without the written permission of the publisher.

For complete copyright information, please see the online version of this work:

<http://www.enotes.com/everyday-law-encyclopedia>