Juvenile Computer Crime - Hacking: Criminal and Civil Liability

Helen W. Yee
Juvenile Computer Crime—Hacking: Criminal and Civil Liability

by HELEN W. YEE*

I
Introduction

Computer systems represented an intellectual challenge to seven Milwaukee teenage boys. Armed with home computers, modems, and limited computer programming knowledge, they invaded the electronic data processing systems of over sixty commercial and governmental institutions during a six to eight month period. Among the systems they penetrated were the computers at a cement company in Canada, a consulting firm in Dallas, Security Pacific Bank in Los Angeles, Memorial Sloan-Kettering Cancer Center in New York, and Los Alamos National Laboratory.1 Their incursions ended only when the Federal Bureau of Investigation discovered their activity and confiscated their equipment.2

What these teenagers did was not an isolated incident.3 As com-

* Member, Third Year Class; A.B., University of California at Berkeley, 1976; M.L.S., University of California at Berkeley, 1978. This note is dedicated to the memory of my father, a Chinese immigrant who placed his dreams in the United States public education system.


2. See supra note 1.

puter literacy and the availability of terminals in homes and schools have increased, juveniles ranging from thirteen to eighteen have entered the realm of computer crime, by unlawfully entering the electronic files of banks, the sensitive defense records of the federal government, the medical research data files of hospitals, and the computerized ticket information of airlines.

Computer crimes committed by juveniles have largely been confined to "hacking," defined as the unauthorized electronic accessing of another's computer system without the intent to defraud or to steal any "property" within the data base. Those who engage in such conduct are known as "hackers."

This note examines the problem of juvenile computer crime, describes existing federal and state criminal laws available to punish and deter hackers, and analyzes why these statutes are inadequate to deal with the problem. The note then proposes civil liability as

vaded TELENET's Telemail System, the international computer message network, with damage estimated between $500,000 and $1,000,000. The Defense Department's computer files may also have been penetrated; Stone, Young Computer Whiz Freed from Charges, San Francisco Chron., Sept. 3, 1983, at 2, col. 1 (teenager raided high school computer, causing $450 in damage); D. PARKER, FIGHTING COMPUTER CRIME 140-43 (1983) (15-year-old male arrested for destroying student computer programs in the University of California's UNIX system); id. at 144-47 (four 13-year-old students at a New York high school raided the computer systems of 21 organizations in the United States and Canada); id. at 148-52 (two high school students played "cat and mouse" with DePaul University officials, threatening to crash the college's system if access to a special computer file was not given; damage amounted to $22,000).

4. Testimony of Oregon Rep. Ron Wyden in Hearings on Computer and Communications Security and Privacy, supra note 1, at 5 (stating that with the computerization of society, the United States is witnessing "the development of a new concept of lawbreaking. One of its most tragic and profound implications is that it attracts some of the brightest young people who seem to fail to recognize the ethical and moral implications of their actions."). See also Testimony of Donn Parker in id. at 75, and in Federal Computer Systems Protection Act: Hearings on H.R. 3970 Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 97th Cong., 2d Sess. 51 (1982) [hereinafter cited as Hearings on H.R. 3970].


Computer experts distinguish between benign hacking and malicious hacking. Benign hacking is the use of computer files which one does have authority to enter, while malicious hacking is considered criminal conduct and is the intentional and unauthorized access of another's computer that has resulted in "various acts of vandalism such as destroying or contaminating data or use of computer service." Hearings on Computer and Communications Security and Privacy, supra note 1, at 74 (testimony of Donn Parker). This note's references to hacking are to malicious hacking.

an alternative to criminal prosecution in curbing teenage hacking, and evaluates the feasibility of this suggested remedy.

II

The Problem: Hacking

Most juveniles view hacking as a game, with any data system that a teenager may access via a telephone being the playing field. Law enforcement agencies, in contrast, view hacking as a crime of breaking and entering into another's property, with the computer being the instrumentality of the crime. Security experts consider it comparable to joyriding in another's car.

Security experts have been surprised at how easily hackers have accessed their systems. The teenage hacker can penetrate a system with only "a home computer, a modem (an inexpensive device that allows computers to transmit data over the phone lines), and a modicum of computer literacy." Once the juvenile is online, he or she can roam at will, traveling across state lines and international boundaries.

Although this activity has received much attention, particularly in the print media, within the last few years, some individuals have questioned the seriousness of juvenile hacking, arguing that the media has sensationalized the problem. Indeed, the prevailing public view is of hacking as high school antics, and of the hackers as pranksters who will eventually grow up. Juvenile hackers

---

10. Marbach, supra note 1, at 43.
11. The Milwaukee teenagers, who dubbed themselves the "414s" because of the area code in their vicinity, raided computers in California, New York, Texas, and Canada. See supra note 1.
13. Computer Whiz Says It's Easy to Break In, supra note 9, at 6, col. 1; Parents of
have also been hailed as heroes, because of their ability to control machines programmed by adults. When juveniles leave "Trojan Horses" in the system to plague the computer programmer or user, or tell others how to get into various systems undetected, they are often dubbed "whiz kids," or are glorified as "Robin Hoods of the Information Age." Both juveniles and adults admire their "creativity." Adolescents often rationalize their behavior with the argument that computers are inanimate objects, and thus, no real harm can result when they break in and play with the system.16

However, the consequences of this public attitude may be serious. The potential for destruction of significant data, such as medical and financial information, is of great concern to computer users.17 Until now, hacking has caused only property damage. No deaths or personal injuries have resulted from this teenage pastime, but the possibilities of such dangerous consequences do exist.18 On one occasion, for example, hackers entered into the computerized hospital records of intensive care patients and increased the dosage of prescribed medication by one hundred percent. If a nurse had not spotted the increase, death to several

 hackers have defended their children as "exuberant, innocent pranksters." D. PARKER, supra note 3, at 148-52.

 14. "Trojan Horses" are additional instructions or modifications introduced into computer programs. These additions or changes are executed "along with normal and expected activity." D. PARKER, supra note 3, at 84. Hackers believe that the results caused by their "Trojan Horses" will not be detected and will be received as "routine output." Id. "Trojan Horses" can be inserted so cleverly that their presence in a program can go unnoticed. It "could require many days or weeks of an expert programmer's time" to find their locations if their "presence were suspected." Id. at 86. These additions or modifications can be segregated from "innocuous-looking data" in such a way that they can be easily erased after they are used. Id. In such a situation, a programmer would have to find "the instructions that [created] the instructions that performed the ultimate unauthorized act." Id. "Trojan Horses" can also be camouflaged "as inconspicuous little subprograms or data that look as if they have some other, legitimate purpose." Id. Apart from "Trojan Horses," programmers can also be plagued by other "[u]nauthorized covert methods of altering the processing in computers." Id. at 84. These include altering input data ("data dildling"), using system anomalies ("trapdoors"), and "changing the order in which functions are to be performed or repeating functions" ("asynchronous attack"). Id.

 15. Marbach, supra note 1, at 46, 48.


 17. Computer Whiz Says It's Easy to Break In, supra note 9, at 6, col. 1. The potential threat of hacking has even forced the Pentagon to reevaluate its computer security. Pentagon Tries to Protect Its Computer, San Francisco Chron., Sept. 26, 1983, at 1, 16, col. 1. Some corporations have also taken similar measures. New Wave Computer Crime, supra note 1, at 45.

patients might have resulted.\textsuperscript{19}

The costs of hacking, in terms of data destruction or alteration, disruption of vital services, and wasted computer time, are difficult to assess, especially if the hackers are never detected or apprehended. It has been estimated that hacking damage to computer users ranges from $450 to $500,000.\textsuperscript{20} In actuality, the true losses are incalculable because computer users do not want their customers and the general public to know that their systems have been penetrated. Some financial and corporate institutions do not even report computer intrusions for fear of losing business.\textsuperscript{21} The amounts of damages from these unreported entries have therefore been left undisclosed. In addition, computer crime, as a new phenomenon, has only recently gained significant attention from those likely to keep such statistics, such as security experts and law enforcement officials.\textsuperscript{22}

Some claim that frequent change of the computer system's passwords may be sufficient to deter juvenile computer perpetrators.\textsuperscript{23} Such measures, however, may inhibit only the weak-hearted hacker, and may "intensify the security battle and offer new challenges to determined hackers."\textsuperscript{24} Hacking is an addictive game; the more challenging it is, the more fascinating the competition

\begin{flushleft}
\textsuperscript{19} Id. \\
\textsuperscript{20} When Robert Nelson, Jr. crashed his high school's computer, it cost $450 to restore the system. Stone, \textit{supra} note 3, at 2, col. 2. The damage caused by the six teenagers arrested by the FBI on October 14, 1983, was estimated at a minimum of $500,000. \textit{Crackdown on computer data tapper}, San Francisco Examiner, Oct. 14, 1983, at A3, col. 2. When the Milwaukee 414s' intrusion destroyed the Memorial Sloan-Kettering Cancer Center's "users account file," the teenagers cost the center about $1500 in revenue. \textit{Computer whiz kids broke up cancer patients' monitoring system}, San Francisco Examiner, Aug. 18, 1983, at A8, col. 4. \\
\textsuperscript{22} Recent attention has been focused on computer crime because of the growing dependence on computers to store information by businesses and government organizations. Sokolik, \textit{supra} note 5, at 359. The growth of computer literacy has also added to this concern. More and more students are being taught to use computers. Approximately 100,000 computers were in U.S. schools in 1982, roughly one for every 400 students. By 1985, it is estimated that there will be 300,000 to 650,000 computers in schools. Golden, \textit{Here Come the Microkids}, \textit{TIME}, May 3, 1982, at 53-54. As a result of this growing computer literacy, it is predictable that juvenile computer crime will increase. \\
\textsuperscript{24} \textit{Computer Whiz Says It's Easy to Break In}, \textit{supra} note 9.
\end{flushleft}
against the system becomes. The ultimate mastery is the defeat of the security system.

Although there are high security systems, such as scramblers and "special keys containing built-in microchips that can be programmed with secret codes" to prevent unauthorized entry, these security measures are presently affordable only to the military, banks, and other large corporate institutions, and remain beyond the financial means of most small businesses, nonprofit medical facilities, and local public institutions. Wells Fargo Bank, for example, allocates in excess of eleven million dollars a year on security, and Grumman Aerospace calculated that over one million dollars will be spent "in hardware alone for encryption devices in order to protect [its] data as it goes out on the telecommunication lines," as well as "additional money in [the] form of people to put up software packages for protection of the data within the system."

Others have argued that the hacking problem should be resolved by educating the potential hacker, rather than by resorting to the legal process. One suggestion has been that computer ethics, including the idea that use of another's data base is stealing, should be taught to the young. It has been suggested further that the potential dangers of hacking should be stressed. The lessons of computer ethics, however, may prove fruitless as long as adolescent hackers are hailed as heroes. Juvenile computer crime will only be deterred when there is public censure of the conduct and a corresponding adequate legal regulation of this activity.

25. Golden, supra note 22, at 52; D. PARKER, supra note 3, at 131.
28. Hearings on Computer and Communications Security and Privacy, supra note 1, at 490 (statement of Jack L. Hancock, Senior Vice President of Wells Fargo and Company).
29. Id. at 495 (statement of Julius Cohen, Director of Technology, Information Resource Management Department, Grumman Aerospace Corporation).
31. Marbach, supra note 1, at 48.
32. Legal regulation and punishment of this misconduct will be a signal to teenagers that hacking is no longer socially acceptable. See War Declared on Computer Invaders, San Francisco Chron., Feb. 2, 1984, at 10, col. 1.
The Existing Computer Crime Statutes

Thirty-three states have computer crime laws. Congress enacted a federal statute only recently. Nevertheless, the current state and federal computer-related crime statutes do not adequately address the problem of teenage hacking.

A. State Law

1. Attributes of the State Computer Crime Statutes

Thirty-three states have enacted computer crime statutes, all since 1978. Some states adopted their computer crime laws in reaction to the growing opportunities for fraud, theft, and destruction of financial instruments, data and other assets contained in the data bases of government and financial institutions.

---


34. See infra notes 75, 88-89.


36. Florida and Georgia legislatures expressed this specific intent to combat such white collar crime in their statutes. See FLA. STAT. ANN. § 815.02 (West Supp. 1983); GA. CODE
Another impetus for the enactment of such legislation was the desire to supplement the traditional laws against theft, embezzlement, larceny, and fraud by wire, in which there were loopholes through which computer crimes might slip. For example, it has been suggested that the Colorado legislature passed its computer crime statute in reaction to the state supreme court's decision in *People v. Home Insurance Co.* In that case, the state's highest court held that no theft was involved in the procurement over a wire of confidential medical information concerning hospital patients, without physical removal of any of these records from the hospital, because confidentiality is not a "thing of value" within the meaning of the theft statute. Absent the legislature's action, the theft statute might well have proved inapplicable to the case of an electronic intruder entering into a computer system and looking at confidential files. It is likely that the Colorado statute was enacted to cover such a possibility.

The state computer crime statutes are generally similar to each other, with a few notable variations. One difference is the mens rea required for conviction. The jurisdictions use a variety of terms to describe what state of mind is required to establish a violation. Thus, Arizona requires that the offender act "intentionally," while Florida forbids criminal conduct performed "willfully, knowingly," and Colorado merely uses the term "knowingly." The California and New Mexico statutes, requiring a higher standard of proof than the other states, reach actions done "maliciously." None of the computer crime statutes pro-

---


40. Id. at 262, 591 P.2d at 1037.

41. *Hearing on S. 240, supra* note 37, at 12-13 (statement of J.D. MacFarlane).

42. Id.

43. See generally *supra* note 33.

44. Id.


vides further definition of these terms. Their meanings must be gleaned from the state’s general statutory definitions for criminal culpability or the jurisdiction’s case law.

In general, “intentionally” can be defined to mean that the person entered the computer system without authorization and with the purpose of causing the result or of engaging in the conduct. “Willfully” can be defined as synonymous with either “intentionally” or “knowingly,” depending on the state’s statutory scheme or case law. A computer invader acts “knowingly” when he or she is aware that the conduct is practically certain or reasonably certain to cause the result that is prohibited by the computer crime statute. If “knowingly” is defined as knowledge that is “reasonably certain,” rather than “practically certain,” direct proof that

49. See generally supra note 33.
50. See infra notes 51-56 and accompanying text.
51. In its general statutory explanations of criminal intent terms, Arizona defines “intentionally” to mean “with respect to a result or to a conduct described by a statute defining an offense, that a person’s objective is to cause that result or to engage in that conduct.” ARIZ. REV. STAT. ANN. § 13-105(a) (Supp. 1982).
52. A Florida court of appeal in Rozier v. Florida, 402 So. 2d 539, 542-43 (Fla. Dist. Ct. App. 1981), defined “willfully” when used in a general intent crime, such as trespassing, to mean that “the entry or remaining [was done] intentionally, knowingly, and purposefully.” The Rozier court found knowledge to be a component of the mens rea required. Id. Therefore, “willfully, knowingly” as used in the Florida computer crime statute has the same meaning as “willfully.” See also State v. Buffett, 397 So. 2d 1060, 1061 (Fla. Dist. Ct. App. 1981) (the court in this grand theft case found “[i]t . . . difficult to see that the addition of the word ‘knowingly’ to the requirement of ‘with intent’ adds anything to the statute. Putting the two together, ‘knowingly with intent’ seems to be a mere repetition.”). Using these arguments, it can be concluded that “willfully, knowingly” means “willfully.”
53. Florida case law also treats “intentionally” and “willfully” synonymously. See Rozier, 402 So. 2d at 542-43. See also Linehan v. State, 442 So. 2d 244, 247 (Fla. Dist. Ct. App. 1983).
54. Under Utah law, “wilfully” has the same definition as “intentionally.” UTAH CODE ANN. §§ 76-6-703, 76-2-103(1) (Supp. 1983). A person acts “[i]ntentionally, or with intent or willfully with respect to the nature of his conduct or to a result of his conduct when it is his conscious objective or desire to engage in the conduct or cause the result.”
55. Under the Colorado statute,
[a] person acts “knowingly” . . . with respect to a result or to a circumstance described by a statute defining an offense when he is aware that his conduct is of such nature or that such circumstances exists. A person acts “knowingly” . . . with respect to a result of his conduct, when he is aware that his conduct is practically certain to cause the result.
COLO. REV. STAT. § 18-1-501(6) (1978). In Colorado, “knowingly” has the same definition as “willfully,” but differs from “intentionally.” Id. According to the Colorado Supreme Court, “knowingly” is the second highest level of criminal culpability. People v. Deressa, 867 P.2d 1353, 1357 (Colo. 1993). “Intentionally” is the highest level of criminal culpability in Colorado. See COLO. REV. STAT. § 18-1-501(5) (1978). “A person acts ‘intentionally’ or ‘with intent’ when his conscious objective is to cause the specific result proscribed by the statute defining the offense.” Id. This culpable mental state is applied only to specific in-
the person knew that the act was illegal is not necessary; it may be inferred from the facts using a reasonable person standard.44 “Intentionally” may require a slightly higher standard of proof of intent than “knowingly,” depending on the jurisdictional definitions.45 A computer perpetrator behaves “maliciously” if he or she has a wish to vex, annoy, or injure, or the intent to do a wrongful act described by the computer crime law.46

The states vary in their classification of computer offenses as misdemeanors or felonies, and in the prison terms and fines they impose.47 In some states, the amount of theft or damage plays an


45. See supra note 53.

46. California defines “malicious” intent as the “wish to vex, annoy, or injure . . . or an intent to do a wrongful act, established either by proof or presumption of law.” CAL. PENAL CODE § 7(4) (Deering 1971). This latter state of mind is more difficult to prove than the others. For example, the District Attorney’s Office in Santa Clara County, California, was unable to bring charges against an 18-year-old hacker who had raided a high school’s computer, because the office could not prove that the boy had entered the system “maliciously” to access or damage school records. Stone, supra note 3, at 2, col. 1. If the statute had required the conduct to be done “intentionally” or “knowingly,” the prosecutor’s case would have been stronger. The juvenile admitted to “knowingly” accessing the school’s electronic data file. He claimed that his intent had been to enter the school’s online system in order to create a better security system. Id. col. 2. In response to this situation, the California legislature recently amended and expanded its computer crime statute. The statute continues to require that the conduct be done “maliciously” when fraud is involved but requires that the violator act only “intentionally” when the conduct does not involve fraud. CAL. PEN CODE § 502 (Deering 1985).

47. Note, Addressing Computer Crime Legislation: Progress and Regress, 4 COMPUTER/ L. J. 195, 203 (1982). For example, the North Dakota law makes no distinction in classification. All computer crimes are felonies, and anyone found guilty under this law may be subjected to a maximum ten-year jail sentence or $10,000 fine, or both, for a Class B felony, or a maximum five years in prison or a fine no greater than $5000, or both, for a Class C felony. N.D. CENT. CODE § 12.1-06.1.08 (Supp. 1984).

In contrast, the Colorado statute classifies computer offenses as either misdemeanors or felonies, and thus permits more gradation of the offenses. COLO. REV. STAT. § 18-5.5-102(3) (Supp. 1982). It provides that if the damage is less than $200, the offense is a misdemeanor. Id. The court may impose a prison term between three months and twelve months, or a fine between $50 and $1000, or both. COLO. REV. STAT. § 18-1-106 (Supp. 1982). If the damage is $200 or more, the court will hold the offender liable for a felony. COLO. REV. STAT. § 18-5.5-102(3) (Supp. 1982). Colorado law prescribes a prison term from two to eight years for computer felonies. COLO. REV. STAT. § 18-1-105 (Supp. 1982).
important factor in determining both the length of imprisonment or the amount of fine. In other states, punishment is determined by the type of computer crime that has been committed, for example, fraud, trespass, invasion of privacy, and/or theft of computer services. A few states have not enacted separate computer crime statutes, but have amended their larceny or fraud and theft laws to encompass illegal access and use of computers.

2. State Law Application to Hacking

The state computer crime statutes cover a variety of computer offenses ranging from "schemes or artifice to defraud or extort or . . . [obtain] money, property, or services," to intentionally entering, accessing, modifying, eliminating, destroying, or damaging data in a computer file, without authorization. Although these state laws were initially designed to reach potential professional computer criminals, such as computer bank robbers, and possibly computer saboteurs and spies eliciting trade secrets from data bases, juvenile hacking does fall within the statutes. Ostensibly, the hacker fits the description of one who "intentionally," "willfully [and] knowingly," "knowingly," or "maliciously" accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data.

The recently enacted Virginia statute and the amended California law specifically focus on hacking. The Virginia law expressly makes several important aspects of hacking—computer trespass, computer invasion of privacy, and theft of computer services—a

---

58. See, e.g., Colorado, Minnesota, Utah, and Iowa statutes, supra note 33.

59. For example, the Virginia statute breaks down computer crime into several categories, including computer fraud, trespass, invasion of privacy, and theft of computer services. VA. CODE §§ 18.2-152.1-152.14 (Supp. 1984). Delaware has two types of computer crime: fraud and misuse. Both types are considered felonies, although of differing degrees. DEL. CODE ANN. tit. 11, § 858 (Supp. 1982). New Mexico labels the illegal activity as either computer fraud or unauthorized computer use. N.M. STAT. ANN. §§ 30-16A-1 to -4 (1982). North Carolina divides computer crime into four types: (1) unauthorized computer access, (2) damaging computers and related materials, (3) denial of computer services to an authorized user, and (4) extortion. N.C. GEN. STAT. §§ 14-453 to -457 (1981).

60. See Massachusetts's amended larceny statute, MASS. GEN. LAWS ANN. ch. 266, § 30 (West 1984), and Ohio's amended fraud and theft statute, OHIO REV. CODE §§ 2901.01, 2913.01 (Page Supp. 1984).

61. See generally supra note 33, particularly the California and Delaware statutes.

62. See supra text accompanying note 36.

63. See supra note 33, to see the similarity of the computer crime statutes of Arizona, New Mexico, Delaware, Georgia, Michigan, Tennessee, North Dakota, South Dakota, Missouri, and Wyoming. See also supra notes 45-48.
Similarly, the California computer statute was amended to cover juvenile hacking with the inclusion of the following provision: "Any person who intentionally and without authorization accesses any computer system, computer network, computer program, or data, with knowledge that the access was not authorized, shall be guilty of a public offense."65

While the state computer crime statutes contemplate hacking, they inadequately address juvenile computer crime. With few exceptions, such as the California and Virginia statutes, most of the state laws were primarily enacted not to prevent juvenile hacking, but rather to deal with professional computer criminals who commit financial fraud, embezzlement, and theft.66 Since hacking is not considered as harmful as computer fraud or theft,67 there has been an apparent reluctance to prosecute juveniles under statutes specifically designed to punish adults for serious computer crimes.68

While the criminal penalties of most state statutes may need adjustment to reflect hacking's relatively less serious nature in relation to other computer offenses, they must also remain sufficient to deter the activity. States could follow the examples set by California and Virginia, whose statutes provide only fines in some cases of computer crime, such as computer "browsing" and invasion of privacy.69

Since only thirty-three states have enacted computer crime legislation,70 several states provide no protection.71 When a teenage hacker sits at a terminal in a state with a computer crime statute and enters a system in another jurisdiction without statutory pro-

---

64. VA. CODE §§18.2-152.4 to 152.6 (Supp. 1984).
66. See supra text accompanying note 36.
67. See supra text accompanying notes 8-16.
68. It may be considered harsh to sentence a teenager to two to four years for "knowingly" accessing a computer system and causing $500 worth of damage when the system crashes, as the Colorado law requires. COLO. REV. STAT. §18-5.5-105 (Supp. 1982). The result could be even worse in Delaware, where "intentional" computer misuse is a Class E felony, punishable by several years imprisonment, or in Rhode Island, where such computer abuse could result in up to five years in prison or a $5000 fine, or both. DELA. CODE ANN. tit. 11, § 858 (Supp. 1982); R.I. GEN. LAWS § 11-52-5 (Supp. 1983).
70. See supra note 33.
71. New York, Texas, and Kansas, for example, have no computer crime statutes.
tection, he or she has committed a crime only in the state with the computer crime statute.\textsuperscript{72} If that jurisdiction fails to prosecute, the other state which has no computer crime law may not assert territorial criminal jurisdiction.\textsuperscript{73} If the communication occurs between a terminal and data base both of which are located in separate states without computer crime legislation, the juvenile cannot be prosecuted in either state.\textsuperscript{74}

B. Federal Law

When juvenile hacking crosses state lines and thereby interferes with interstate commerce, those jurisdictions without applicable computer crime, theft, or wire fraud statutes may look to federal law. Although federal legislation had been introduced as early as 1977, Congress only recently enacted a federal computer crime statute.\textsuperscript{75}

Prior to the enactment of this statute, interstate computer offenses had been prosecuted primarily under the Federal Wire Fraud Statute,\textsuperscript{76} which provides for the prosecution of anyone who devises a "scheme or artifice to defraud," to take under "false or

\textsuperscript{72} Most of the state statutes do not discuss where the computer crime must occur in order for a state to have competent jurisdiction. See generally supra note 33. However, at least one state, Connecticut, in its recently enacted computer statute, addressed this issue. Act of May 31, 1984, Pub. Act No. 84-206, 1984 Conn. Pub. Acts. In sum, the offense is deemed to have been committed in Connecticut if "any act performed in furtherance of the [computer crime] occurs in this state or if any computer system or part thereof accessed in violation of [the statute] is located in this state." Id. § 12.

See also W. LAFAVE & A. SCOTT, JR., HANDBOOK ON CRIMINAL LAW 117-25 (1972), for a discussion of territorial criminal jurisdiction. Under the common law territorial theory of jurisdiction, a crime had only one situs, namely "where the vital act or result occurred," and that only the place of situs had jurisdiction. Id. at 118-19. In a number of states, statutory extensions of territorial jurisdiction have abolished this common law notion. Thus, some states by statute may assert "jurisdiction to punish conduct within the state causing a bad result to occur outside the state." Id. at 122. See, e.g., OHIO REV. CODE ANN. § 2901.11 (Page 1982); CAL. PENAL CODE § 778a (Deering 1983); ILL. ANN. STAT. ch. 38 § 1-5 (Smith-Hurd 1972).

\textsuperscript{73} Generally, if no state statute makes a conduct illegal, and such conduct is not considered a common law crime, there is no crime to prosecute. W. LAFAVE & A. SCOTT, JR., supra note 72, at 57.


\textsuperscript{76} 18 U.S.C. § 1343 (1976). Although 40 federal statutes have been identified as conceivably applicable to computer related crime, the Federal Wire Fraud Statute is more commonly used because most computer crime occurs over a wire. Hearing on S. 240, supra note 37, at 51, 161.
fraudulent pretenses, representations, or promises," the money or property of another "by means of wire, radio, or television communication in interstate or foreign commerce." Such a convicted offender shall be "fined not more than $1,000 or imprisoned not more than five years, or both." For several reasons, the Federal Wire Fraud Statute is and was an inadequate solution to the juvenile hacking problem. First, it is difficult to prove the requisite mens rea. Hacking does not entail the intent to defraud or to obtain money; teenagers instead seek entertainment when they penetrate electronic data bases.

The establishment of intent is difficult. When a hacker intentionally accesses a computer system, he or she is also using another's valuable computer time. This value vests the computer time with a property-like aspect. Therefore, the intent to use another's computer time is arguably equivalent to the intent to take property. This analogy works only if it is established that the hacker knew of the "fraudulent nature" of his act. As previously noted, however, neither hackers nor the general public commonly perceive hacking as "fraudulent."

Another problem with using the Federal Wire Fraud Statute is that the computer cases that have been prosecuted under this law have generally involved actions in which the defendant used the

77. Id.
78. Id.
80. Cancer Hospital's Computer Invaded—'Just for Thrills,' supra note 8, at 13, col. 1.
81. Although state courts have refused to "regard the use of a computer as a property interest" where no statute specifically defines computer time as such an asset, the "[f]ederal courts have taken an expansive approach and view computer time and services as property subjected to theft." Comment, Legislative Issues in Computer Crime, 21 Harv. J. on Legis. 239, 251-52 (1984).
83. See supra text accompanying note 13.
data base for financial gain. Therefore, there may be no solid precedent for prosecution where entry is for recreational enjoyment, and law enforcement officials may be reluctant to file charges.

Finally, the penalties available under the Federal Wire Fraud Statute may be inadequate and inappropriate to the conduct. The maximum fine of $1,000 is inadequate punishment to compensate fully the victim's losses. Also, as with the state statutes, the ungraded prison sentence could prove too harsh to impose on a convicted teenage hacker, even if first time offenders would receive only one year in prison. Any federal jail sentence, regardless of the length, may be viewed as overly punitive to impose on a juvenile, in view of the current social acceptance of teenage hacking.

With computers permeating all aspects of American society—records management, banking, marketing, law enforcement, and national defense—and the growing potential for computer abuse, as demonstrated by the antics of the computer hackers, congressional concern about the adequacy of existing federal laws to cope with computer crime has increased. Congress's concern prompted the passage of the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984" (1984 Act), after three earlier attempts.

84. For example, in United States v. Seidtitz, 589 F.2d 152 (4th Cir. 1978), the defendant accessed the computer system of his former place of employment to copy a multi-million dollar software program for use at his own computer firm. See also United States v. Muni, 668 F.2d 87 (2d Cir. 1981); United States v. Gioveno, 637 F.2d 941 (3rd Cir. 1980).


86. See supra note 89, regarding the reluctance of imposing ungraded criminal penalties against amateurs, and supra text accompanying note 13, concerning the social acceptance of teenage hacking.


The 1979 Act (like its predecessor, the 1977 Act) was criticized on several grounds: (1) the statute provided for an unnecessary expansion of "federal jurisdiction into areas traditionally reserved for the States"; (2) the incidence of computer crime did not warrant a federal statute; and (3) the proposed law exposed individuals to criminal liability for possible innocent conduct, such as accidental entry. Hearing on S. 240, supra note 37, at 3 (statement of J.D. MacFarlane). Even supporters of the 1979 Act, including private industries, government agencies, and legal professionals, recognized the validity of these criticisms. Id. at 108-29, 138-52. The American Bar Association (ABA) strongly recommended that the stat-
The statute makes it illegal for anyone to "knowingly" access a computer without authorization\(^90\) for any of three purposes: (1) to "disclose" and "use" information about the country's "national defense or foreign relations, or any restricted data, as defined in paragraph r of section 11 of the Atomic Energy Act of 1954," with the intent to injure the United States or to give any foreign nation an advantage; (2) to obtain "information contained in financial records of a financial institution," as defined by the Right to Financial Privacy Act of 1978, or "contained in a file of a consumer reporting agency on a consumer," as defined by the Fair Credit Reporting Act; or (3) to knowingly modify, destroy, or prevent the use of data in any computer "operated for or on behalf of the Government of the United States."\(^91\)

\(^90\) The 1981 proposed legislation adopted many of these suggestions, especially those from the ABA. It included provisions for concurrent federal/state jurisdiction, with published guidelines precisely defining when the federal government could exercise jurisdiction. Hearing on S. 240, supra note 37, at 113 (resolution of the ABA). The ABA also resolved that a five-year maximum prison sentence for all offenses covered under the 1979 Act would be more reasonable than a 15-year maximum penalty that was devoid of "any structure of gradation to guide the exercise of the sentencing authority." Id. n.2. A 15-year sentence could prove too severe, especially if applied to amateurs or first time offenders. Id. at 113. The Electronic Funds Transfer Association (EFTA) further recommended that the act be amended to guarantee that only wrongful access and not accidental entry would be punished, and that such wrongful entry should be a misdemeanor. Otherwise, EFTA feared that the "severe level of penalties in the bill might actually dissuade reporting of wrongdoing. Scaling the criminal penalty should overcome such resistance." Id. at 139 (recommendations of EFTA). The EFTA also suggested that "if fines and money damages were made available to the injured party, reporting would be encouraged." Id.

\(^91\) See also H.R. REP. No. 894, 98th Cong., 2d Sess. 20 (1984). Unauthorized access also prohibits employees who have authorized access from entering a computer "for purposes to which their authorization does not extend." Act of Oct. 12, 1984, supra note 75, at 2190-91.
Congress tailored the statute precisely. It protects the financial, personal, medical, and employment information contained in the computerized files of U.S. government agencies, financial institutions regulated by federal law, and consumer reporting agencies that furnish consumer information to third parties by "means or facility of interstate commerce." 92

While Congress meticulously described what was to be protected under the new law, it left the issue of federal preemption ambiguous. Originally, the 1984 Act contained a provision addressing the concerns of state and local authorities over the expanding powers of the federal government, 93 but at the last moment, this clause was deleted from the final version of the new statute. 94 However, legislative history seems to indicate a willingness to defer to local authorities, and to "use the [f]ederal investigative and prosecutive arms . . . to [deal] with interstate operations that cannot be handled effectively because of the limitations of process in local jurisdictions." 95

The activities engaged in by juvenile hackers clearly fall within the new federal computer crime statute. 96 For example, the seven Milwaukee teenagers who knowingly accessed the Memorial Sloan-Kettering Cancer Center's data base containing credit information about its patients would have been in violation of the new law. If prosecuted and found guilty under this statute, they could


The Fair Credit Reporting Act covers consumer reporting agencies who furnish their information to third parties by means or facility of interstate commerce. Consumer records contain not only credit information, but also personal, employment, and medical data as it relates to a consumer's credit. 15 U.S.C.A. § 1681a (West 1982).

93. The provision stated that "[the statute did] not prohibit any lawful authorized investigatory, protective or intelligence activity of a law enforcement agency of the United States, a state, or a political subdivision thereof, or an intelligence agency of the United States." 130 CONG. REC. S14445-46 (daily ed. Oct. 11, 1984). Even this provision was not as definitive as the clauses in the 1981 Act and the 1983 Act, because it failed to spell out precisely when federal jurisdiction could have been exercised, or whether such jurisdiction was to be held concurrently. Compare the language in H.R. 3970, 97th Cong., 1st Sess. (1981) and H.R. 1092, 98th Cong., 1st Sess. (1983) with the terms proposed for the 1984 Act.


95. Hearing on Computer Crime, supra note 23, at 29-30 (Statement of John Keeney, Deputy Assistant Attorney General, Criminal Division, Department of Justice). Floyd I. Clarke, Deputy Assistant Director, Criminal Investigative Division, FBI, agreed with Keeney's statements. Id. at 30.

have faced "a fine of not more than the greater of $5,000 or twice the value obtained or loss created by the offense or imprisonment for not more than one year, or both." 97

Given the severity of the penalties provided in the 1984 Act, there has been some hesitation in prosecuting juveniles. 98 Furthermore, because of the confidentiality requirements of juvenile criminal proceedings, the successful prosecution of a teenage hacker may go unnoticed by other potential violators. 99 Therefore, criminal sanctions may be of minimal value in deterring juvenile hacking.

The solution to the problem of curbing hacking may lie in imposing civil liability. Because federal authorities may hesitate to criminally prosecute, federal legislation providing for civil causes of action may be more effective. Moreover, the possibility of monetary compensation may provide motivation for computer victims to file suit. 100

IV
Possible Civil Liabilities

Civil liability serves a dual purpose: deterrence and compensation. If teenagers know that they will be personally liable to compensate victims for the damage they cause, they may be dissuaded from invading the computer systems of others. A victim, unwilling to criminally prosecute a juvenile, may be willing to seek civil redress and restitution. 101

Currently, only three states, Virginia, California, and Connecticut, grant statutory civil relief for injury caused by unauthorized computer access. 102 The Virginia law provides that "[a]ny person whose property or person shall be injured by reason of a violation of any provision [of this statute] may sue therefor and recover for any damages sustained, and the costs of suit. Without limiting the generality of the term, 'damages' shall include loss of profits." 103 The California statute states: "[T]he owner or lessee of the com-

98. See supra text accompanying note 86.
100. See EFTA's suggestions supra note 89.
101. Id. See also Note, Misappropriation of Computer Services: The Need to Enforce Civil Liability, 4 COMPUTER/L. J. 401 (1983).
103. VA. CODE § 18.2-152.12 (Supp. 1984).
puter system . . . may bring a civil action against any person . . . for compensatory damages, including any expenditure reasonably and necessarily incurred" to make sure that the computer system and the information contained within has not been "altered, damaged, or deleted by the access." The California law also holds the parents of an emancipated minor responsible for their child's conduct, but only if there has been a conviction. It also permits the court to award attorney's fees to a successful plaintiff. The recently enacted Connecticut law allows a victim to file a suit in equity if the aggrieved party reasonably believes "that any other person has been engaged in an alleged violation of any provision of [the statute]." Equitable remedies available under this law are: (1) injunctive relief, (2) restitution, and (3) receivership. The victim may also bring an independent action for damages, or such a damage claim may be brought in conjunction with a suit in equity.

Although most states do not have such similar statutes, civil remedies may nonetheless exist. Generally, a child can be held liable for his or her own negligent or intentional act. Since few teenagers are independently wealthy or financially solvent, however, filing a private cause of action against a minor tortfeasor may prove fruitless. If the juvenile's parents are joined in the action, the theory of vicarious parental liability, statutorily codified in all fifty states, imputes the juvenile's conduct to his or her parents.

105. Id.
106. Id.
108. Id.
109. Id.
parents.\textsuperscript{113}

Some of the state statutes not only make parents liable for the damage to person and property, but also hold them responsible for the thefts committed by their children.\textsuperscript{114} The statutes are all similar in scope. They will not impose vicarious liability for negligent acts, instead requiring either "willful" or "malicious" behavior by the juveniles.\textsuperscript{115} In addition, most of the statutes require that the

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{113} See supra note 112. The ceiling amounts range from $500 to $5000. \textit{Id.} at 586-87.
\item \textsuperscript{115} See supra note 112.
\end{enumerate}
\end{footnotesize}
minors must have been under the control and custody of the parents or guardians at the time of the misconduct.\textsuperscript{116}

The victim of juvenile hacking may prevail in a suit brought under the parental liability laws, if he or she can prove: (1) the juvenile’s “willful” or “malicious” intent to do the delinquent act,\textsuperscript{117} or in California, “willful misconduct,”\textsuperscript{118} and (2) actual damage to property or theft as a result of the intent.\textsuperscript{119}

To prove “willful” intent the plaintiff must show both the intent to do the wrongful act that caused the damage, and the intent to damage.\textsuperscript{120} A juvenile who intentionally and without authorization accesses a system to alter or to purposefully destroy the computerized records has the requisite “willful” intent. To prove “malicious” intent or “willful misconduct,” however, one must demonstrate the following: “(1) the intentional doing of something with knowledge (expressed or implied) that serious [damage] is the probable (as distinguished from the possible) result, or (2) the intentional doing of an act with a wanton and reckless disregard of its consequences.”\textsuperscript{121} Therefore, if a hacker knows that his or her conduct will probably result in the destruction of valuable information stored in a data base, but continues to trespass into the system in total disregard of this danger, and the system is damaged as a result, this activity can be characterized as “willful misconduct,” and thus, he may be found to have harbored “malicious” intent.\textsuperscript{122}

Finally, since computer information, storage, and time have been held to be property,\textsuperscript{123} if the juvenile hacker can be shown to

\textsuperscript{116} Id.; see also Note, Constitutional Law—Constitutionality of Legislative Imposition of Vicarious Parental Liability for Delinquent Acts of Juveniles, 12 BALTIMORE L. REV. 171, 172-73 (1982). Generally, a parent has control and custody of the child if the minor is under 18 years old, is unemancipated, and resides with the mother or father. See vicarious parental liability statutes of Arkansas, Colorado, Delaware, Illinois, Kansas, Kentucky, Mississippi, and South Dakota supra note 112.

\textsuperscript{117} See supra note 112.

\textsuperscript{118} CAL. CIV. CODE § 1714.1 (Deering Supp. 1985).

\textsuperscript{119} See supra note 112.


\textsuperscript{122} Note, supra note 120, at 750.

\textsuperscript{123} See supra text accompanying note 81.
have damaged or stolen any of these items with the requisite intent, a hacker's parents may be held liable under the vicarious liability statute. They would be held responsible for compensating the victim up to the amount of the damage or the liability limit of the state statute, whichever figure is less.\textsuperscript{124}

If intent cannot be proven, however, because the hacker behaved negligently, the victim may pursue claims against the parents under other tort theories. For example, the injured party may assert that the parents acted negligently in their control and supervision of the misbehaving adolescent. Parental negligence may be difficult to prove; ordinary prudence\textsuperscript{125} would not likely prevent a parent from giving his or her child a computer or allowing the child to use a terminal without supervision. Moreover, liability cannot be established by proving that the parents entrusted their child with a dangerous weapon,\textsuperscript{126} except in the unlikely event that a computer is found to be a dangerous instrument.\textsuperscript{127} Therefore, in the absence of proof of parental negligence, or agency, or public acceptance that a computer is a dangerous instrument, a victim of hacking cannot obtain compensation from the parents if the child has acted only negligently.

In sum, the application of vicarious parental liability to hacking is limited.\textsuperscript{128} It is only viable where the child acts intentionally or maliciously. States appear disinclined to impose vicarious liability for negligent acts.

What is needed to effectively deter teenage hackers is a specific statute that would hold juveniles civilly liable or, in the case of an unemancipated minor, that would hold the parents vicariously liable for any injury, including personal harm and property damage,

\begin{itemize}
\item \textsuperscript{124} See supra text accompanying notes 112-13.
\item \textsuperscript{125} A person acts with ordinary prudence when his behavior conforms with the "community ideal of reasonable behavior, determined by the jury's social judgment." W. KEETON, PROSSER AND KEETON ON THE LAW OF TORTS 175 (5th ed. 1984).
\item \textsuperscript{126} See Note, supra note 120, at 750-51, for an explanation of what is meant by "entrusting a child with a dangerous instrumentality," an act for which a parent can be held liable in limited situations. See also CAL. CIV. CODE § 1714.3 (Deering Supp. 1985).
\item \textsuperscript{127} However, consider the following: Floyd I. Clarke analogized that a computer was "much like a gun, a knife." Ferraro, supra note 9, at 1, col. 3. When teenage hacking results in personal injuries or death, the public may reconsider its thinking.
\item \textsuperscript{128} A problem also arises when one tries to execute a judgment obtained under one state's vicarious liability statute in another state, because of limitations in the long-arm statute of the state where judgment was issued. See Memorial Lawn Cemeteries Ass'n v. Carr, 540 P.2d 1156 (Okla. Sup. Ct. 1975). Cf. Indiana Ins. Co. v. Pettigrew, 115 Cal. App. 3d 862, 171 Cal. Rptr. 770 (1981).
\end{itemize}
caused by a juvenile’s knowing unauthorized access into another’s computer system. Under such a law, a victim could sue for compensatory damages, including losses in computer time and services, and costs of employing personnel to verify that the records in the data base have not been modified, damaged, or deleted. Although the California statute\textsuperscript{129} is similar to this recommendation, it focuses on property damage,\textsuperscript{130} and restitution is available only when there is a criminal conviction.\textsuperscript{131} The California law is also ambiguous as to what intent is needed to sustain a civil action. While the criminal section of this statute requires that the criminal activity be conducted “maliciously” when it involves credit information and “intentionally . . . with knowledge” for any other unauthorized access,\textsuperscript{132} civil actions are conditioned on successful criminal prosecution and are linked to the vicarious parental liability statute which mandates “willful misconduct” on the part of the minor.\textsuperscript{133} Although the civil relief encompassed in the Virginia law is also similar to the statute suggested by this note, it does not impose vicarious liability on the parents of juvenile hackers.\textsuperscript{134} This is also true for the recently enacted Connecticut law.\textsuperscript{135}

\textbf{V}

\textbf{Conclusion}

As American society has become more computer literate and more dependent on electronic data processing systems, juveniles have become involved in computer crime, especially in the form of hacking. In the absence of ethical instruction to accompany basic computer education, and in light of the reluctance of the public to call for the criminal prosecution of juveniles, hacking will likely continue. Where the criminal law falters, victims of juvenile computer crime should look to civil remedies to discourage misconduct and to recover their losses. State lawmakers should assist their endeavors by passing such appropriate legislation as vicarious parental liability statutes allowing victims of juvenile hackers

\begin{itemize}
  \item \textsuperscript{129} \textit{Cal. Penal Code} § 502 (Deering Supp. 1985).
  \item \textsuperscript{130} \textit{Id.}
  \item \textsuperscript{131} \textit{Id. See also Ohio Rev. Code Ann.} § 2151.35.5 (Page Supp. 1984). The Ohio statute provides that a delinquent convicted of computer fraud or theft may be required to make restitution for property damage as a condition of probation.
  \item \textsuperscript{132} \textit{Cal. Penal Code} § 502 (Deering Supp. 1985).
  \item \textsuperscript{134} \textit{Va. Code} § 18.2-152.12 (Supp. 1984).
\end{itemize}
to recover in civil suits independent of criminal prosecution. The vacuum in the existing computer crime laws should not remain.