Fall 1993


Glenn D. Baker

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

http://repository.jmls.edu/jitpl/vol12/iss1/4

This Comments is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
TRESPASSERS WILL BE PROSECUTED:
COMPUTER CRIME IN THE 1990s

by GLENN D. BAKER*

I. INTRODUCTION

Michelangelo! There was a time when the mention of this name would bring up thoughts of an outstanding 14th century artist whose claim to fame was the "Sistine Chapel." This all changed in March 1992, when a computer virus of the same name threatened to destroy data on an estimated 60 million personal computers in the world, thereby sending multitudes of businesses scrambling for anti-virus programs. While the virus did not wreak the havoc many predicted, it still accomplished some damage and caught the attention of many in the populace who never considered the effect this type of problem could have on our nation. In the past, few would ever consider a "computer criminal" in the same regard as other felons. Ken Citarella, assistant district attorney for Westchester County in White Plains, New York, has commented that "[c]omputer crime just doesn't stack up against murder." Perhaps this is the reason that the government has not dealt with this problem as quickly as some would like.

Meanwhile, an accounting firm has placed the cost of computer crime to businesses at 3 to 5 billion dollars per year. This may be a conservative estimate, as it does not possibly take into account all of the computer crime that goes unreported by companies who are reluctant to report these crimes for fear that the publicity would hurt stockholder

* Law Student, Georgia State University; B.B.A. 1984, Adelphi University; Former Special Agent in the Criminal Investigation Division of the U.S. Treasury Department (Internal Revenue Service).


3. Rosenblatt, Deterring Computer Crime, TECHNOLOGY REV., Feb. 1990, at 34 (estimate made by the accounting firm Ernst & Young). See also Alexander, Not-so Spectacular Computer Crimes by Not-so-Surly Criminals, COMPUTERWORLD, Aug. 13, 1990, at 54. Some in the industry argue that there is no accurate way one could measure or even estimate how much computer crime costs, since so few crimes are reported. See infra text accompanying note 4.
confidence, and the belief that police involvement is inconsequential since the crime is so difficult to prove.\textsuperscript{4} The crimes are being committed by a wide diversity of individuals—not just those involved in the industry. It is not relegated to the "computer geeks" one would normally conjure as an image when contemplating computer crime. Regular "street criminals" are now involved in this type of crime and are learning the ins and outs of computers.\textsuperscript{5}

Computer crime has become so serious that it is now a top priority of the Justice Department. In this regard, the department has set up a computer-crime unit in the criminal division of its attorneys offices, and in the Federal Bureau of Investigation [hereinafter F.B.I.].\textsuperscript{6} The United States Attorney General, William P. Barr, has called computer crime "one of the top three of our white-collar priorities."\textsuperscript{7} Some, however, argue that not enough is being done to combat this crime. Kenneth Rosenblatt, a deputy district attorney for Santa Clara, California says that "I think what it is going to take is people dying, unfortunately, before anything will be done about computer crime."\textsuperscript{8}

That computer crime has become a serious threat to our nation cannot be disputed. Even more serious, however, is that it has become the "weapon of choice" among white-collar criminals.\textsuperscript{9} It has been deemed similar to "any other form of theft, except that it's more subtle and it's more sophisticated."\textsuperscript{10} As an aide to former Attorney General Richard Thornburgh said: "It was just a matter of time before criminals discovered the advantages of computers. . . . Computers make it increasingly possible to get propriety information at financial institutions and other firms."\textsuperscript{11} What is constantly debated is how our nation should respond

\textsuperscript{4} Id.
\textsuperscript{5} Weixel, Futurists, COMPUTERWORLD, Jan. 4, 1988, at 47.
\textsuperscript{6} Gertz, Computer Criminals Draw Federal Focus, WASH. TIMES, Sept. 19, 1992, at A3. See infra note 252 for a discussion of the privacy issues relating to the actions of these task force groups.
\textsuperscript{7} Id.
\textsuperscript{8} Alexander, supra note 2.
\textsuperscript{9} Quintanilla, Computer Crimes Newest Nemesis for Regulators, Police Departments, INVESTOR'S DAILY, Mar. 9, 1990, at 25.
\textsuperscript{10} Potts, 'Hacker' Pleads Guilty in AT&T Case; Sentence Urged for Maryland Man Among Stiffest Yet for Computer Crime, WASH. POST, Mar. 23, 1991, at A1, quoting Assistant U.S. Attorney Geoffrey R. Garinther. Garinther was involved in the prosecution of a 32 year old man, Leonard Rose Jr., who obtained computer information that would have enabled him to modify the telephone giant's software program which contained instructions that would actually tell other computers what to do. Rose was eventually caught and arrested in a Secret Service sting operation called "Operation Sun Devil." This, and other similar operations, has come under much criticism by First Amendment activists. For a discussion of First Amendment and privacy issues relating to computer crime, see infra text accompanying note 252.
\textsuperscript{11} Id.
to these crimes in the future and whether or not the Federal and State laws we now have in place are sufficient to deter the perpetrators from committing these crimes.

This paper will examine the current Federal statute (18 U.S.C. § 1030) that deals with computer crime. It will discuss the history of the statute, the major elements of the statute, and its effectiveness in combatting and deterring computer crime. It will also discuss proposed amendments to the statute, what changes to the statute we may see in the future as a result, and what impact computer viruses such as Michelangelo, which are relatively new to this area of law, will have on all of the above. This paper will also discuss the only published case that has been prosecuted thus far under this statute. In addition, this paper will examine instances where the arrest of computer "hackers" and other users has led to First Amendment privacy issues, and the reason so many other computer-related cases have been prosecuted under federal statutes other than the computer statute.

II. HISTORY OF THE STATUTE

A. EARLY LEGISLATION

"The prosecution of white collar crime, which silently robs millions of dollars from all of us, must remain in high priority for Federal law enforcement. It is in this perspective we must deal with computer fraud as we attempt to deter the theft of one of our most prized intangible commodities, information." As Congressman Peter Rodino indicated in a 1986 speech before the House of Representatives, computer crime is white collar crime and should be combatted as such by the federal government. In 1977, a United States Senator from Connecticut, Abraham Ribicoff, first introduced a computer crime bill to Congress, the Federal Computer Systems Protection Act [hereinafter FCSPA], which sought to make the prosecution of computer crimes easier by using extremely broad language. While the bill was never passed, it did plant the seed for future legislation in Congress.

Ian Murphy has gained fame as the "computer consultant" for the 1992 Universal Studios theatrical release, Sneakers, a film about com-

15. Wilson, Viewing Computer Crime: Where Does the Systems Error Really Exist?, 11 COMPUTER/L.J. 265, 268 (1991). The proposed statute stated that any "knowing, willful manipulation or attempted manipulation of a computer, computer system, computer network or any part thereof..." would be considered a crime and could have a jail sentence of up to 15 years.
puter spies doing undercover work for what they believe to be the National Security Agency.\(^{17}\) In 1982, however, Murphy was involved in a scheme that created dummy corporations and ordered thousands of dollars worth of computer equipment.\(^ {18}\) He was arrested and convicted of receiving stolen property, but since there was no federal computer crime law at the time, he only received a third-degree felony count, was fined $1,000, ordered to do 1,000 hours of community service and given 2\(1/2\) years of probation.\(^ {19}\) Murphy's mother felt the penalty should have been stiffer and went to her Congressman, Larry Coughlin, to discuss the situation.\(^ {20}\) Coughlin eventually raised the issue on the floor of Congress in 1983 and Congress passed a national computer crime law the following year,\(^ {21}\) entitled the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the 1984 Act).\(^ {22}\)

The 1984 Act was intended to protect computers and computerized information.\(^ {23}\) It prohibited the accessing of computers in three areas. The first section of the 1984 Act made it a felony to knowingly access a computer without authorization for the purpose of gaining information relating to United States defense or foreign relations with the intent of causing injury to the United States or giving an advantage to a foreign nation.\(^ {24}\) The second section made it a misdemeanor to knowingly access a computer without authorization to obtain financial information contained in the record of a financial institution or a consumer reporting agency.\(^ {25}\) The statute also made it a misdemeanor to knowingly ac-

\(^{17}\) Goodman, *Hacker for Hire; Real-life Sneaker Ian Murphy puts the Byte on Corporate Spies*, PEOPLE, Oct. 19, 1992 at 151.

\(^{18}\) Id.

\(^{19}\) Id.

\(^{20}\) Id.

\(^{21}\) Id.


\(^{24}\) 1984 Act, *supra* note 22, § 1030(a)(1) (current version at 18 U.S.C. § 1030(a)(1) (1988)). The text is as follows:

(a) Whoever—

(1) knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data . . . of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.

\(^{25}\) Id. § 1030(a)(2) (current version at 18 U.S.C. § 1030(a)(1) (1988)). The full text is as follows:
cess a computer without authorization in order to use, modify, destroy or disclose information in or prevent the authorized use of the computer with the knowledge that the computer is operated for or on behalf of the United States and would affect the government’s operation of the computer.\textsuperscript{26}

The 1984 Act contained penalties of up to ten thousand dollars or imprisonment of up to ten years for the most serious first time offender of the classified information subsection and penalties were increased for repeat offenders of this subsection, with a maximum of twenty years imprisonment and a one hundred thousand dollar fine.\textsuperscript{27} The misdemeanor offenses carried a penalty of five thousand dollars or imprisonment for not more than one year.\textsuperscript{28}

The new statute came under some harsh criticism. Most felt that it was too vague and limited in scope.\textsuperscript{29} In fact, from the time of its inception until it was amended in 1986, only one person was indicted under the 1984 Act.\textsuperscript{30} In that case, a Los Angeles computer hacker, Phillip Gonzalez Fadriquela, was indicted under the 1984 law for using his home computer to gain access to a Department of Agriculture computer system.\textsuperscript{31} The indictment contained seven charges, four misdemeanor charges which were brought under the 1984 Act, two counts of wire fraud and one count of making false statements to a federal agent.\textsuperscript{32} Fadriquela’s major defense was that he was just playing with his computer and did not know he was accessing a government system.\textsuperscript{33} After

\begin{enumerate}
\item (a) Whoever—
\begin{enumerate}
\item knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information contained in a financial record of a financial institution, as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401 et seq.), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq).
\end{enumerate}
\end{enumerate}

\textsuperscript{26} Id. § 1030(a)(3) (current version at 18 U.S.C. § 1030(a)(3) (1988)).

\textsuperscript{27} Id. § 1030(c) (current version at 18 U.S.C. § 1030(c) (1988)).

\textsuperscript{28} Id.

\textsuperscript{29} See, e.g., Tompkins & Mar, The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem, 6 COMPUTER/L.J. 459 (1986). For example, the authors point out that various key words are not defined in the 1984 Act. For a discussion of the absence of definitions in the 1984 Act, see infra notes 37-38 and accompanying text.


\textsuperscript{32} Betts, DP Worker Charged with Hacking; Grand Jury Cites Recent Federal Computer Crime Law, COMPUTERWORLD, Feb. 11, 1985, at 2. For a discussion of the wire fraud statute, see infra notes 192-258 and accompanying text.

\textsuperscript{33} The Region, supra note 31.
a plea bargain, Fadriquela pleaded guilty to three misdemeanors for wire fraud, and in return, the government dropped all other charges.\textsuperscript{34} He was sentenced to three years of probation, fined $3,000 and required to perform 200 hours of community work.\textsuperscript{35} In addition, Fadriquela had to forfeit all his computer equipment and issue a statement which explained how he committed the offenses.\textsuperscript{36}

Despite the fact the 1984 Act played a major role in the conviction of Fadriquela, it actually had very little impact and received ample criticism. The major criticism was that the 1984 Act did not “define key terms or clearly outline the investigative and jurisdictional aspects of the legislation.”\textsuperscript{37} For instance, the only defined term in the statute was “computer.” Other key terms such as “access,” “use,” and “without authorization,” were omitted.\textsuperscript{38} In addition, it left access to private computers and computer networks unaffected and excluded other financial data such as tax returns.\textsuperscript{39} This difficulty with the 1984 Act led to the passage of the Computer Fraud and Abuse Act of 1986 (the 1986 Act).\textsuperscript{40}

\section*{B. The 1986 Act}

The 1986 Act amends the 1984 Act and substantially changed the way in which computer crime could be prosecuted. In addition to changing the 1984 Act, the 1986 Act added three new crimes, providing it with six definitions of computer crimes.\textsuperscript{41} The Judiciary Committee

\begin{itemize}
  \item \textsuperscript{34} Korzeniowski, \textit{Agencies' Hacker Troubles Blamed on Bulletin Board; Users, Vendors Facing up to Break-Ins}, \textit{Computerworld}, July 8, 1985, at 1.
  \item \textsuperscript{35} Id.
  \item \textsuperscript{37} Wilson, \textit{supra} note 15.
  \item \textsuperscript{38} Tompkins, \textit{supra} note 30. See also Betts, \textit{U.S. Attorneys Push to Clarify Vague '84 DP Crime Law}, \textit{Computerworld}, July 1, 1985, at 22. Fadriquela's attorney also charged that the law's language was vague, because the term “affect” was not defined. He argued that it was unclear what “affecting a government computer means,” and that “if it covers the act of entering an access code without authorization, it's like being charged with tapping on a door without ever going behind it.”
  \item \textsuperscript{39} Ray, \textit{supra} note 23.
  \item \textsuperscript{41} Id. § 1030(a)(1)-(6). The 1986 Act contains the following six definitions of crimes relating to computers:
    \begin{enumerate}
      \item Knowingly accessing a computer without authorization and obtaining information protected against disclosure by the United States with the intent to use that information to the injury of the United States.
      \item Intentionally accessing a computer without authorization and obtaining information in a financial record of a financial institution, credit card information or credit reporting information.
      \item Intentionally accessing any computer of a department or agency of the United States without authorization where the computer is exclusively for the
COMPUTER CRIME

[hereinafter the Committee] which enacted the bill was concerned that the new statute would be too broad.42 It sought to limit Federal jurisdiction to situations where there was a compelling Federal interest, such as the use of Federal computers, involvement of financial institutions, or an interstate crime.43 There was a uniform belief that most other computer related crimes could and should be handled by private industry.44 Some also believed that the individual States should handle such crimes.45

In any event, the new act contained several significant changes to the 1984 Act and three new additions.46 The 1986 Act replaced some of the previously criticized awkward language in subsections (a)(1) and (a)(2). For example, "having accessed a computer without authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" was replaced by the simpler "or exceeds authorized access," which is now defined in Section (e)(6).47

The 1986 Act also expanded the "protection of financial institutions to all customers rather than only to customers who [were] 'individuals' or partnerships consisting of five or fewer partners" under subsection (a)(2), by broadening the terms "financial institution" and "financial record"48 in order to protect computerized credit reports and other computerized information relating to an individual's relationship with a financial institution, thereby maintaining privacy.49


MIN. NEWS 2479, 2482.
43. Id.
44. Id.
47. See S. REP. NO. 432, supra note 42, at 2486.

after Hughes statement].
49. See S. REP. NO. 432, supra note 42, at 2484.
The statute also made subsection (a)(3) a “pure trespass provision,” by making unauthorized access (of a computer used exclusively by or for the U.S. government) alone a criminal offense under subsection (a)(3) and repealing the so-called “use exemption.” The legislative history illustrates that this change was enacted due to Justice Department concerns that the 1984 Act may have required a showing that the computer information accessed was ‘used, modified, destroyed, or disclosed,’ rather than just proving a mere trespass. Congress was also quick to point out that there would be no liability in “insider” cases where an individual is authorized to use a computer in his or her department, yet uses another for which he or she lacks authorization. The motivation for this was to protect “whistleblowers” who may disclose information they have obtained from a government computer.

The statute also amends subsections (a)(2) and (a)(3) by changing the scienter requirement from “knowingly” to “intentionally.” The scienter requirement for subsection (a)(1) remains “knowingly.” The legislative history indicates the Committee changed the scienter requirement from “knowingly” to “intentionally” for two reasons. First, it was not interested in prosecuting those who made careless mistakes and thereby gained access to a computer without intending to do so. Second, Congress believed that “knowingly” was not an adequate standard when dealing with cases involving computer technology, since it would not prevent an individual who accidentally gains access to information in a computer he or she has permission to use, yet is not authorized to access certain information from and does so only by mistake, from being held liable. The focus should be on those who have a “clear intent” to enter computers without proper authorization.

The major impact of the 1986 Act was in its three new offenses. The first, under subsection (a)(4), was designed to penalize thefts of property by the use of a computer which occurred as a result of a scheme to defraud, and was the first federal computer fraud offense

50. Hughes Statement, supra note 48, at H3276.
51. Tompkins, supra note 30. See infra notes 53-54 and accompanying text for a discussion of the “use exemption.”
53. Id. at 2485.
54. Id.
58. Id.
59. Id.
60. Id.
61. Hughes Statement, supra note 48, at H3276.
created by Congress. Congress emphasized that the use of a computer or computers had to be a major part of the scheme to defraud, not just incidental. Also, it wanted to make clear that acts of trespass which cause a loss of computer time, and are misdemeanors under subsection (a)(3), should be distinguished from acts of fraud for purposes of subsection (a)(4), which are punishable as felonies. For instance, a person could commit a trespass under the statute by unauthorized access into another's computer for only a minute. The Committee clearly did not want every act of unauthorized entry into a government computer, no matter how brief the access, to be a felony. In fact, the legislative history is filled with comments relating to the new statute by members of both the Senate and the House, indicating that they wished it to be narrow in scope and to proceed slowly and cautiously. To further make the distinction between computer trespass, a misdemeanor, and computer fraud, a felony, the Committee emphasized that the scienter requirement of the latter crime, "knowingly and with intent to defraud" is based on the standard used in the federal credit card fraud statute.

The second new crime, under subsection (a)(5), has been labeled a "'malicious damage' felony violation in regard to Federal interest computers, if there is damage of $1,000 or more." This section makes it a felony to intentionally access a Federal interest computer without authorization, and alter, damage or destroy information within the computer or prevent authorized use of the computer. This subsection is aimed at " outsiders," those who have no permission whatsoever to access a Federal interest computer. The subsection focuses on two circumstances where it will penalize "outsiders:" first, where there is a loss to any victim of $1,000 or more in a single year. The Committee set this high amount to prevent felony charges against every small operator who may modify another's computer data in some insignificant

63. Note, supra note 46, at 478.
64. See S. Rep. No. 432, supra note 42, at 2486.
65. Id. at 2487-89.
66. Id. at 2488.
67. See, e.g., 132 Cong. Rec. S14455 (daily ed. Oct. 1, 1986) (statement of Sen. Denton) ("[T]he bill . . . does not represent the furthest possible reach of Federal jurisdiction in this area: it is not intended to. It is the general belief of the sponsors of this bill and of the Department of Justice that in this rapidly changing area of computer technology, the best legislative approach is to proceed cautiously . . . .").
72. Id.
73. Id.
These individuals can still receive misdemeanor-level penalties under subsections 1030(a)(2) or 1030(a)(3); second, the subsection will penalize "outsiders" when there is alteration, damage or destruction of data relating to medical care and treatment. The legislative history indicates that Congress wanted to pay particular attention to the altering of medical treatment records. This is deemed so serious, given the potential for life-threatening harm as a result of such conduct, that a showing of a $1,000 loss is not needed for this part of the subsection.

The third new crime, established under subsection (a)(6), is aimed primarily at "hackers" who use "pirate bulletin boards" and penalizes those who traffic in any password without authorization if the trafficking effects interstate commerce or is used by or for the United States Government. The general consensus has been that the 1986 Act was a massive improvement over the 1984 Act and it cured many of the deficiencies of the 1984 Act. It addresses many more forms of computer crimes. The language has been simplified and it is more sensibly structured and definite in meaning. It clarified concepts such as "property" and "privacy" and how they relate to computer technology, and educated potential abusers, thereby putting them on notice. In addition, the 1986 Act enhanced, without question, the potential for de-

74. Id.
75. Id.
76. Id. at 2490.
77. Id.
78. Id. The legislative history provides an example of this where a group of youngsters known as the "414 Gang" gained access into the computer system of a major New York hospital specializing in cancer treatment. This gave them access to the radiation treatment records of over 6,000 cancer patients. While there were no financial losses at stake, the thought of these adolescent criminals having access to, and the potential for, change of a cancer patient's treatment is both scary and absurd. Id. at 2480.
79. Hughes Statement, supra note 48, at H3276. See Branscomb, Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, 16 RUTGERS COMPUTER & TECH. L.J. 1, 11 n.46 (1990). "Hacker is a term which has developed various meanings. In the media it is often used in a derogatory manner because of the detrimental consequences of some of the 'hacking.' The term has been used in the press to mean skilled computer professionals or students with an intent to perpetrate an antisocial act of theft, embezzlement, or destruction. However, the original use within the computer community was laudatory to describe highly skilled and dedicated computer programmers."
Id.
80. See S. REP. NO. 432, supra note 42, at 2491. " 'Traffic means to transfer, or otherwise dispose of, to another, or to obtain control of with intent to transfer or dispose of such passwords.' " Id.
82. See generally Tompkins, supra note 30, at 44; Note, supra 46, at 40.
83. Tompkins, supra note 30, at 44.
84. Note, supra note 46, at 490.
However, fewer than 250 cases relating to computer crime have been prosecuted in the past decade, so while the potential for deterrence was certainly enhanced by the 1986 Act, it is questionable whether or not a prosecution rate so low can actually have any deterrent value. Furthermore, some offenders are actually rewarded for their crimes by companies who will actually hire them as “security consultants.”

As the above illustrates, while the 1986 Act was an improvement over the 1984 Act, it is clearly far from perfect and has certainly received its share of criticism. For instance, although the 1986 Act did simplify a lot of the language, it still left key terms, such as “computer” and “access,” undefined. It also does not provide for any civil remedies and while the potential for a substantial jail term exists, the comparable financial penalty does not seem adequate. The 1986 Act also does not address the alteration or destruction of computer programs if the damage is not greater than one thousand dollars and has no effect on medical care. Therefore, an individual who has accessed a Federal interest computer without authorization and has received something of intangible value, such as computer data and use, to which the government cannot put a dollar value, may be able to argue he or she has not violated the statute. Perhaps most importantly, critics have argued that the Act’s drafters did not foresee the advent of computer viruses like Michelangelo, so the act does not completely address the specific conduct involved in the proliferation of computer viruses.

---

85. Id. at 486.
86. Rosenblatt, supra note 3.
87. Id. One example is that of a 14-year-old offender who said he committed the computer crime in order to get the victim or another company to hire him. Id.
88. Wilson, supra note 15, at 272.
89. Id. For example, 18 U.S.C. § 1030(c) provides for a maximum jail term of twenty years, but the fine referred is only one thousand dollars. With some estimating the average take for a computer crime at four hundred thirty five thousand dollars, the one thousand dollar fine seems inconsequential and most important, not much of a deterrent. Id. at n.49.
90. Ray, supra note 23, at 477.
91. Id. at 477-78, 486.
92. Tramontana, Computer Viruses: Is There a Legal Antibiotic?, 16 Rutgers Computer & Tech. L.J. 253, 266 (1990). “A computer virus can be defined as ‘a program which can insert executable copies of itself into other programs.’” Id. at 255. For a discussion of computer viruses, See infra text accompanying notes 287-328. But see United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (an individual who created a computer worm was convicted under the 1986 Act). For a full discussion of this case, see infra notes 121-71 and accompanying text.
III. THE CASES

The first time an individual was brought to trial and convicted under the 1986 Act was in February 1989, when an eighteen-year-old high school dropout was sentenced to nine months in prison with no opportunity for parole and was fined ten thousand dollars. In 1988, Herbert Zinn of Chicago, who used the code name "Shadow Hawk," was arrested and was originally charged with violations of six counts of 18 U.S.C. § 1030(a)(4) to (6), including unlawfully invading computers belonging to NATO, Bell Labs, and the United States Air Force and stealing 52 AT&T software programs from them with an estimated worth of $1.18 million.

As the cases below illustrate, Zinn's relative youth is not surprising. An AT&T spokesperson called his actions "yuppie vandalism." Ironically, the Assistant U.S. Attorney who prosecuted the case said that while he was preparing for the case, he turned to his nine year old son to show him how to use a computer. During the proceedings, the United States Attorney cited white-collar crime studies and movies such as War Games as social barometers whose messages regarding the acceptability and excitement of these actions needed to be reversed. The prosecution could not use the full extent of the law in this case due to the age of the defendant. If Zinn had been an adult, he could have faced up to twenty years in a federal penitentiary; however, a sentence that severe is almost inconceivable in a case such as this when one compares it to similar cases.

Another one of the first individuals to be charged and convicted under the 1986 Act was Kevin David Mitnick, who was arrested late in

---


94. Boucher, supra note 93.

95. Wilson, supra note 15, at 279-80. Although Zinn did access the computer and its stored data without authorization, he did not damage or destroy the computer. Id. at 282.

96. Boucher, supra note 93.

97. Id.

98. Kane, "Sorcerer's Apprentice" Meets Less Benign Fate, NAT'L J., Feb. 5, 1990, at 8. The Assistant U.S. Attorney on the case, William J. Cook of Chicago, stated that "[t]he kids are much more knowledgeable. You just have to swallow your pride and kneel down at the knees of your son." Id.


100. Id. at 281.

101. He was only 16 and 17 years old when he committed the computer fraud for which he was convicted. See Branscomb, supra note 79, at n.91.

102. Wilson, supra note 15, at 281.
December 1988. Mitnick was a colorful figure who went by the code name "Condor," was listed under the telephone directory as "James Bond," and had "007" as the last three digits of his telephone number.

Prior to his conviction, Mitnick had a history of numerous encounters with law enforcement and corporate security officials. This time he was charged on four counts of computer fraud under 18 U.S.C. § 1030, including stealing programs valued at one million from the Digital Equipment Corporation and using unauthorized MCI long-distance service codes to avoid telephone charges while accessing computer systems at Leeds University in England. Digital also reported that it would cost the firm more than $4 million in downtime and reworking of its software to repair the damage Mitnick had done.

Mitnick was treated as a hardened criminal after his arrest. He was denied bail by the judge and not allowed to make phone calls for fear that he may gain access to a computer over the telephone lines. He was held in a high-security detention center since the court ruled him "a risk and danger to the public." The prosecutors called Mitnick a person who could do as much damage with "a computer terminal as a bank robber with a gun."

The sentencing judge apparently agreed with this assessment. United States District Court Judge Mariana Pfaelzer rejected a plea bargain agreement, despite the fact the prosecutors told the judge they found no evidence that Mitnick ever damaged computers he accessed or attempted to make any money from the software he illegally purloined.

104. Id. Based on the Robert Redford movie character in the film "Three Days of the Condor," who outwits the government. Id. Ironically, over a decade after the "Condor" movie was made, Robert Redford appeared in a movie specifically dealing with espionage—"Sneakers." See supra note 17 and accompanying text.
105. Id.
107. Rebello, supra note 106.
108. Markhoff, supra note 106.
109. Id.
111. Id.
113. Savage, Hacker Prosecution; Suspect Held, Denied Phone Access by District Court, COMPUTERWORLD, Jan. 9, 1989, at 2.
114. Johnson, supra note 103.
from private computer banks, and he did not destroy any computer or implant a virus into anyone's computer. This was not enough evidence to convince the judge to go along with the plea bargain. She stated to Mitnick that "you have been engaging in this conduct for too long, and no one has actually punished you. This is the last time you are going to do this."

Mitnick was finally sentenced to one year in prison, six months in a residential treatment program and three years of probation. This was the first instance where an individual was tried and convicted under the 1986 Act section (a)(6) which makes it a crime to gain access to an interstate computer network for criminal purposes. It was, according to the Justice Department, the "stiffest sentence a hacker has received."

The most prominent and significant prosecution of a "hacker" under the 1986 Act was in United States v. Morris. In Morris, the defendant was found guilty following a jury trial of violating 18 U.S.C. § 1030(a)(5)(A). He was sentenced to three years probation, four hundred hours of community service, a fine of ten thousand fifty dollars and the costs of his supervision. He became the first person convicted by a jury of a felony under the 1986 Act.

In the fall of 1988, Robert Morris was a first year graduate student studying computer science at Cornell University. He had significant computer experience through his undergraduate work at Harvard University. At Cornell, he was given explicit authorization to use computers in the Computer Science Division.

---

115. Murphy, supra note 112.
116. Id.
117. Id.
120. Supra note 118.
121. Morris, 928 F.2d at 504.
122. Id. at 506.
123. Id.
125. Morris, 928 F.2d at 505.
126. Id.
127. Id.
In October 1988, Morris devised a scheme to create a program which would later be called the INTERNET “worm.” He wanted the worm to spread widely, yet draw little attention to itself, so he programmed it to be difficult to detect so other programmers could not “kill” it easily. Morris released the worm from a computer at Massachusetts Institute of Technology on November 2, 1988. The worm worked much better than Morris anticipated and actually replicated and reinfected machines at a faster rate. When Morris recognized the damage that was being done, he sought to stop the worm by sending out an anonymous message over the network. The network was too clogged, however, and the message did not get through on time to warn programmers how to kill the worm and prevent reinfection. By the time the worm was killed, computers at numerous installations, including leading universities, military sites and medical research facilities, were affected. The worm caused an estimated 6,200 computers to shut down. Estimated labor costs to clear out the memories of the computers and check the software ran from $96 million to as high as $11.1 billion.

According to experts in the field, no actual damage to computer hardware or software occurred. This did not prevent Morris from being indicted and convicted at trial. At trial, Morris testified that his “purpose was to see if [he] could write a program that would spread as widely as possible. The worm spread on the network far faster than I expected.” He said he realized his experiment had turned into a “dismal failure” and that “[it] was a mistake, and [he’s] sorry.” Morris went on to testify that when he first realized the extent of what he had done he “was scared; it seemed like the worm was going out of control.” After his failed attempt at warning programmers, he rejected

128. Id. INTERNET is “a group of national networks that connect university, governmental, and military computers around the country. Id. “A ‘worm’ is a program that travels from one computer to another but does not attach itself to the operating system of the computer it ‘infects’” as opposed to a “virus,” which does attach itself. Id. at n.1.
129. Id.
130. Id. at 506.
131. Id.
132. Id.
133. Id.
136. Id.
137. “Virus” Culprit Convicted, FACTS ON FILE WORLD NEWS DIG., February 2, 1990 at 70.
139. Id.
an idea to write a second program to kill the first: "I didn’t do that because I had messed up with the first one and it didn’t appear that I would be able to do any better the second time." \[140\]

In his defense, Morris’ lawyer played a videotape of the defendant giving a lecture at the National Security Agency in 1987 on how to gain access to computers illicitly. \[141\] Ironically, Morris’ father is the Chief Scientist of the National Computer Security Center and is a nationally recognized and highly respected expert on computer break-ins. \[142\] He has actually testified before Congress in the past on the subject of computer viruses. \[143\] Nonetheless, Morris was found guilty and appealed.

On appeal, Morris had two major arguments. First, that the “Government had to prove not only that he intended the unauthorized access of a federal interest computer, but also that he intended to prevent others from using it, and thus cause a loss.” \[144\] Second, Morris argued that the evidence did not prove that Morris had unauthorized access, but rather that he had exceeded authorized access. \[145\] The United States Court of Appeals disagreed with both arguments and upheld Morris’ conviction.

To make its determination regarding Morris’ first argument, the court agreed with Morris that the text was not clear enough to preclude a review of the legislative history of the 1986 Act, despite the fact the District Court ruled the statute was clear and unambiguous. \[146\] Therefore, the court compared the earlier 1984 version (subsection (a)(3) of the 1984 act) \[147\] with subsection (a)(5) of the 1986 Act, which replaced the 1984 subsection. \[148\] The court also examined the legislative history of the 1986 Act in order to determine the intent of Congress in enacting subsection (a)(5). \[149\]

---

140. Id.
143. Id. at 10.
144. Morris, 928 F.2d at 507.
145. Id. at 509.
146. Id. at 506-07.
147. 1984 Act, supra note 22, § (a)(3) (current version at 18 U.S.C. § 1030(a)(5) (1988)). The earlier subsection covered anyone who knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation.
148. Morris, 928 F.2d at 508-09.
149. Id. at 507-09.
COMPUTER CRIME

The court, in reviewing the legislative history, agreed with Morris that the concern of Congress was that it did not want to penalize someone who "stumbled" into someone else's computer by "mistaken, inadvertent, or careless acts of unauthorized access." However, in looking at the intent standard in subsection (a)(5), the court stated that the "wording, structure and purpose" of the subsection illustrates that the "intentionally" standard applies only to the "accesses" phrase of the subsection, and not to its "damages" phrase as Morris argued. Therefore, whether or not Morris intentionally sought to "cause loss" by creating this worm, and the facts clearly indicate he did not, was irrelevant as to whether or not he violated subsection (a)(5).

The court reached its conclusion by comparing the old (1984 Act) statute with the newer one (1986 Act). It noted that the 1986 version changed the "mens rea" requirement from "knowingly" to "intentionally," and did not repeat the requirement after the "accesses" phrase, as did the 1984 Act. In comparison, other subsections in the 1986 Act that were amended did keep the "mens rea" requirement at the beginning of both the "accesses" phrase and "damages" phrase. The court agreed with the prosecution which argued that the decision to state the "mens rea" requirement only once in the new statute, along with the decision to replace the word "knowingly" with the word "intentionally" shows a clear intent to apply the requirement only to the "accesses" phrase. This would satisfy the congressional objective of protecting someone who inadvertently stumbled into another computer by mistake, since it would make the scienter requirement more difficult to satisfy, as knowledge is much easier to prove than actual intent. Hence, with the court's interpretation of the statute, all that would have to be proven was that Morris "intentionally" accessed the computer without authorization.

Morris' second argument maintained that his conduct was, at most, "exceeding authorized access" and did not meet the subsection's definition of "unauthorized access." The court recognized that the congressional intent was for the new subsection to "be aimed at outsiders." The court also noted that this did not preclude a situation where the

150. Id. at 507.
151. Id. at 509.
152. Id. at 508.
153. Id.
154. Id.
155. Id.
156. Id.
157. Id. at 509.
158. See supra notes 70-76 and accompanying text for a discussion of the Congressional intent regarding this subsection of the 1986 Act.
offender's act of trespass was interdepartmental in nature.\textsuperscript{159} For example, a Labor Department employee who uses his department's computers to access an FBI computer without authorization can be criminally prosecuted under the statute.\textsuperscript{160} Such a person would be considered an "outsider" since he or she was not an FBI employee. Likewise, Morris did have authorized access to some federal interest computers (through INTERNET) and would not be considered an "outsider." He was, however, unauthorized to access the federal interest computers into which he released the worm. The court held he did not "exceed authorization" as he contends. Rather, he was totally "unauthorized" to access those particular computers.\textsuperscript{161}

The case, the first of its kind in dealing with computer crime and the 1986 Act, had quite an impact. Many legislators who supported the creation of the 1986 Act were relieved that it proved effective in this case despite the fact the computer worm and virus were unknown at the time the Act was drafted.\textsuperscript{162} This case set the "precedent that a person who creates worms and viruses can be held accountable,"\textsuperscript{163} and answered the question as to whether the 1986 Act was broad enough to cover all aspects of computer crime.\textsuperscript{164} Apparently, it is.

Like the case itself, the sentence that Morris was given\textsuperscript{165} received much publicity and was quite controversial. Frederick J. Scullin Jr., the United States Attorney who announced the sentence in the case, commented that "it was extremely difficult in this case to strike a fair balance between the unique circumstances surrounding Robert Morris' conduct and the goal of deterring future computer-related crime."\textsuperscript{166}

Many in the legal community and computer industry, however, believe the penalty was not severe enough, and that it would not only fail to deter other "hackers," but might actually encourage other "hackers" who now realize the risk of the penalty is not great enough to outweigh the benefit of the crime, whatever that benefit may be.\textsuperscript{167}

\textsuperscript{159} Morris, 928 F.2d at 510.
\textsuperscript{160} Id.
\textsuperscript{161} Id.
\textsuperscript{162} Nelson, supra note 124.
\textsuperscript{164} Supra note 137.
\textsuperscript{165} See supra note 123 and accompanying text.
\textsuperscript{167} See, e.g., Computer "Worm" Was no Joke; Jail its Creator, NEWSDAY, Jan. 24, 1990. This editorial commented that if this was a situation where someone stole the keys to and broke into a government office, and caused several hundred dollars of lost work time and other damages, he would certainly go to jail. The only difference in the Morris
trict Court Judge had followed the sentencing guidelines, Morris would have faced 21 to 27 months in prison. Others, however, believe that the penalty was severe enough. In any case, the issue is now settled as the Supreme Court has let stand the criminal conviction of Morris by declining to review the case.

The significance of Morris in the area of computer law cannot be emphasized enough, as we may start seeing more and more cases prosecuted under 18 U.S.C. § 1030 in the future, rather than under other federal statutes as has happened in the past. As one publisher of a computer magazine put it, the decision "protects those who are the subjects of computer databases, and at this point that includes every American. It stands for the notion that any intrusion into a system will have criminal consequences, and so it makes every prosecution of these crimes a lot easier. [The case] is extremely important." Whether this is indeed the case remains to be seen. The next section discusses how the government has prosecuted most cases relating to computer crime under federal statutes other than the Computer Fraud and Abuse Act of 1986.

IV. OTHER FEDERAL STATUTES AND RELATED CASES

Prior to Morris, the federal courts had never interpreted nor applied the 1984 Act or the 1986 Act in a published opinion. Despite all the attention the federal computer statute receives, the fact remains that most computer related crimes have been prosecuted under other federal statutes. The potential federal criminal offenses under Title 18 of the United States Code under which computer crimes could be and have been prosecuted, other than The Computer Fraud and Abuse Act, are

169. See, e.g., Alexander, supra note 163. Marc Rotenberg, office director of Computer Professionals for Social Responsibility, commented that “A jail sentence for a person who acted without malicious intent would strike most people as heavy-handed and takes too narrow a view of the problem if you are really trying to reach young hackers.”
are listed below. This is followed by a brief discussion of each statute and how it may be applied to computer crimes, and any relevant cases: Section 641—Stealing a "Thing of Value" from the Federal Government; Section 1029—Fraud and Related Activity in Connection with Access Devices; Section 1341—Fraud by Mail; Section 1343—Fraud by Wire, Radio, or Television; Section 1346—Scheme or Artifice To Defraud; Section 1362—Malicious Mischief—with Government Property; Section 2314—Interstate Transportation of Stolen Property.173

A. SECTION 641

In United States v. Lambert,174 the defendants sold information obtained from a Drug Enforcement Agency (DEA) computer which had details on drug informants and various investigations the DEA was performing.175 They were charged with violating 18 U.S.C. § 641 which prohibits conversion or the unauthorized sale of "any record, voucher, money, or thing of value of the United States or of any department or agency thereof."176

Lambert argued that what he stole was not a "tangible" object and that the computer information itself was not a "thing of value" within the meaning of the statute.177 The District Court held that the computer information was "highly sensitive and confidential," and had an "extraordinary" and "incalculable" value, "so long as it remained in the Government's exclusive possession."178 It was obtained "by the expenditure of countless man hours and other resources" and was "capable of saving lives or, if misappropriated, severely jeopardizing them."179 Therefore, Lambert's motion to dismiss was denied and the court determined his action could come under the statute.180 Under the court's holding, it would appear that Lambert would also support the prohibi-

173. Branscomb, supra note 79, at 45. 18 U.S.C. § 2510—The Electronic Privacy Act and 18 U.S.C. § 2710(a)—Unlawful Access to Stored Communications would also seem to have potential in this area; however, no published cases relating to computer crime have yet been prosecuted under these two statutes. See also Lederman, Criminal Liability for Breach of Confidential Commercial Information, 38 Emory L.J. 921, 977, 982, 985. It is beyond the scope of this article to examine each of these statutes and their elements in detail, yet it is important to note how they have been used to prosecute computer related crime both prior to the 1984 and 1986 Acts, and even after those Acts became law.

175. Id.
176. Id. at 892 n.1 (quoting 18 U.S.C. 641 (1970)).
177. Id.
178. Id. at 895.
179. Id.
180. Id. at 900.
tion of electronic trespass and require computer crime laws to protect the freedom of access to information.\textsuperscript{181}

\subsection*{B. \textsc{Section 1029}}

Under section 1029, "access device" includes any "card, plate, code, account number, or other means of account access that can be used . . . to obtain money, goods, services, or any other thing of value . . . or initiate a transfer of funds."\textsuperscript{182} The scienter requirement is that the act must be done "knowingly and with intent to defraud."\textsuperscript{183} A computer could certainly qualify as an access device. Therefore, one could envision a computer crime prosecuted under this statute.

\subsection*{C. \textsc{Section 1341}}

In \textit{United States v. Curtis},\textsuperscript{184} the defendant was charged with four counts of mail fraud which "prohibits the devising or intending to devise any scheme or artifice to defraud, or for obtaining money by fraudulent representations and using the mails to execute same."\textsuperscript{185} Curtis created a business called the "Computer Matching Institute" which advertised that it could assist individuals seeking dates or marriages by using computerized psychological matching.\textsuperscript{186} Curtis charged a substantial fee for the service without any intent of performance.\textsuperscript{187} He placed ads in various newspapers and sent out questionnaires through the mail to those who answered the ads.\textsuperscript{188} The customer would then forward the form back along with his or her check through the mail.\textsuperscript{189}

The court held that whether or not the scheme itself was a failure or success was irrelevant; it was sufficient that the mail was used to carry out the scheme.\textsuperscript{190} The evidence presented established the two substantive required elements of mail fraud: (1) the act of having devised or intending a scheme to defraud, and (2) the act of willfully and intentionally carrying out an essential step in the scheme to defraud.\textsuperscript{191} Both elements were present in this case, thereby illustrating how a stat-

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{181} Ray, \textit{supra} note 23, at 479.
\item \textsuperscript{182} 18 U.S.C. § 1029 (Supp. V. 1987).
\item \textsuperscript{183} Id.
\item \textsuperscript{184} United States v. Curtis, 537 F.2d 1091 (10th Cir. 1976).
\item \textsuperscript{185} Id. at 1093 (quoting 18 U.S.C. § 1341 (1988)).
\item \textsuperscript{186} Id.
\item \textsuperscript{187} Id.
\item \textsuperscript{188} Id.
\item \textsuperscript{189} Id.
\item \textsuperscript{190} Id. at 1094.
\item \textsuperscript{191} Id.
\end{itemize}
\end{footnotesize}
ute which is facially unrelated to computers can be used to prosecute a crime related to computers.

D. SECTION 1343

This statute is perhaps the most frequently used in prosecuting computer related crimes, other than 18 U.S.C. § 1030.192 In United States v. Seidlitz,193 the defendant was convicted of two counts of wire fraud, under 18 U.S.C. § 1343, which provides that “[w]hoever, having devised or intending to devise a scheme . . . to defraud . . . or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme. . .”194

The defendant was a former employee, responsible for computer security, at a company under contract to operate a computer facility for the Federal Energy Administration.195 After his retirement from the company to start his own business, Seidlitz continued to access the computer system from his home using interstate telephone lines, even though he was no longer authorized.196 The Fourth Circuit Court of Appeals stated that “Seidlitz used the telephone to tamper with and manipulate a machine which was owned by others, located on their premises, and obviously not intended for his use.”197

Seidlitz argued that the computer data he stole was “property in the public domain subject to appropriation by persons such as himself.”198 The court did not agree. Even though the original form of the computer system was available to the public, the fact that the company spent substantial amounts of money to modify the system and protect the system, along with the fact that they now enjoyed a competitive advantage because of their work, permitted a finding that the data was private property of the company, not public.199 The court upheld the conviction.

Seidlitz is important in that the court applied the wire fraud statute to computer abuse by ruling that there is federal jurisdiction over interstate communications under the statute and that computer data is property.200 The case would also seem to allow for private investigations of

192. See Tramontana, supra note 92, at 263.
194. Id. at 153 n.1 (quoting 18 U.S.C. § 1343 (1988)).
195. Id.
196. Id. at 154-55.
197. Id. at 159.
198. Id. at 160.
199. Id.
various computer crimes, such as the spreading of computer worms or viruses.\textsuperscript{201}

In \textit{United States v. Giovengo},\textsuperscript{202} two Trans World Airline (TWA) employees were convicted of two counts of wire fraud.\textsuperscript{203} The two defendants devised a scheme that when a customer would purchase a one-way ticket from TWA, one would give the customer a flight coupon, but would keep the auditor's coupon, any other flight coupons and the passenger receipt.\textsuperscript{204} In order to get the tickets, it was necessary for the defendants to use the airline's computer, which would forward information from Pittsburgh to the main computer in Kansas City.\textsuperscript{205} After receiving his or her coupon, the passenger would go to the boarding gate, where the other defendant would exchange the coupon for a boarding pass, to allow the passenger to get on the plane.\textsuperscript{206} Meanwhile, after the flight departed, the two defendants would put the entire ticket back together, mark it void, and send it to the accounting department which would not look for any amount of cash spent on the ticket, since it had been voided. The two defendants would then pocket the money that the passengers had paid.\textsuperscript{207}

One defendant appealed, contending that § 1343 only applies to those interstate wire communications regulated by the Federal Communications Commission (FCC), and since TWA was not regulated by the FCC, there was no violation of the statute.\textsuperscript{208} The Third Circuit Court of Appeals examined both the statute and the legislative history and held that there is "[n]othing in the language of § 1343 [that] suggests that its scope is limited to fraud committed by use of interstate wires subject to FCC regulation."\textsuperscript{209} Additionally, even if the language were limited to federal regulation, the lines were actually owned and maintained by AT&T who is a common carrier and subject to the jurisdiction of the FCC.\textsuperscript{210}

The court, in upholding the conviction, concluded that "inasmuch as . . . the computer link-up was necessary in order to print the tickets sold to TWA passengers," the use of interstate communications was an essential part of the scheme, and that if the defendants never had access to the computer system in the first place, they could never have suc-

\textsuperscript{201} Id.
\textsuperscript{202} United States v. Giovengo, 637 F.2d 941 (3rd Cir. 1980).
\textsuperscript{203} Id. at 942.
\textsuperscript{204} Id.
\textsuperscript{205} Id.
\textsuperscript{206} Id.
\textsuperscript{207} Id.
\textsuperscript{208} Id.
\textsuperscript{209} Id.
\textsuperscript{210} Id.
ceeded in their scheme to defraud the airline.\textsuperscript{211} It has been suggested that this case supports the notion that the wire fraud statute can be used to prohibit the fraudulent spreading of computer viruses, since viruses may be spread by interstate transmission of computer information over the telephone.\textsuperscript{212} If this were indeed the case, perhaps the outcry to amend the 1986 Act to deal specifically with computer viruses would not be so great.\textsuperscript{213}

In \textit{United States v. Muni},\textsuperscript{214} the defendant was convicted of one count of wire fraud and one count of willfully using a counterfeit credit card.\textsuperscript{215} Muni owned a shoe store and set up a routine Merchant Agreement with Chemical Bank enabling his store to accept VISA and Master Charge cards.\textsuperscript{216} He used counterfeit credit cards to charge two hundred sixty seven fraudulent purchases and withdrew ninety thousand dollars from his account before Chemical Bank discovered the fraud.\textsuperscript{217} In order to perpetrate his scheme, Muni would call the Chemical Bank Authorization Center (CBAC), who in turn would feed this information into a computer which would ascertain whether the card was issued by Chemical Bank.\textsuperscript{218} If it was not, the computer at CBAC would forward an interstate electronic inquiry over the telephone lines in order to get authorization from VISA or Master Charge.\textsuperscript{219}

Muni argued that since all he did was call Chemical Bank, which was located in the same state as his business, he therefore did not transmit or cause to be transmitted any interstate communications. Hence, he could not be prosecuted under section 1343.\textsuperscript{220} The Second Circuit Court of Appeals held that even though Muni did not actually make an interstate transmission, he caused it.\textsuperscript{221} Since it was foreseeable that an interstate computer check for authorization would be performed with respect to a credit card for not issued by a local bank, Muni was in violation of the statute.\textsuperscript{222} Therefore, \textit{Muni} illustrates that a person does not have to actually use a computer in order to be convicted of a computer crime. Reasonable foreseeability that a computer may be used is enough to satisfy the "act" requirement of the crime.

\textsuperscript{211} \textit{Id.} at 944-45.
\textsuperscript{212} Ray, \textit{supra} note 23, at 482.
\textsuperscript{213} For a discussion of the proposed amendment to deal with computer viruses, see \textit{infra} notes 287-328 and accompanying text.
\textsuperscript{214} United States v. Muni, 668 F.2d 87 (2d Cir. 1981).
\textsuperscript{215} \textit{Id.}
\textsuperscript{216} \textit{Id.} at 88.
\textsuperscript{217} \textit{Id.}
\textsuperscript{218} \textit{Id.}
\textsuperscript{219} \textit{Id.}
\textsuperscript{220} \textit{Id.} at 88-89.
\textsuperscript{221} \textit{Id.} at 89.
\textsuperscript{222} \textit{Id.} at 90.
Most recently, in March of 1990, the Secret Service completed a two-year investigation called "Operation Sun Devil," resulting in the seizure of several computer bulletin boards and the indictments of four hackers belonging to a group called the "Legion of Doom." They were arrested due to a scheme where they stole documentation from a Bell South Telephone Company (Bell South) enhanced 911 system. In a case that garnered as much media attention as Morris, one of the hackers who had a prior computer-fraud conviction, Robert Riggs, age 22, pleaded guilty to interstate transportation of stolen property and wire fraud and one count of conspiring to commit computer fraud. Riggs was sentenced to 21 months in jail and fined $233,000 to pay for repairs to the Bell South network. Franklin Darden, 24, pleaded guilty to one count of conspiring to commit computer fraud and was sentenced to 14 months and a comparable $233,000 fine. Adam Grant, 22, pleaded guilty to having 15 or more Bell South access codes with the intent to defraud. He received the same sentence as Darden.

A fourth individual, Craig Neidorf, age 20, an editor of an electronic newsletter called Phrack, was originally charged with six counts in an indictment for wire fraud, computer fraud, and interstate transportation of stolen property valued at $5,000 or more. He did not, however, plead guilty as the others had and his case went on to become a much publicized trial. The allegations against Neidorf were that he and Riggs had devised a plan that would defraud Bell South by stealing a computer text file which contained information relating to its emergency (911) system. The text file specifically detailed the procedures for installation, operation, and maintenance of E911 services, and the government claimed Riggs and Neidorf wanted to obtain it to print this information in Neidorf's newsletter Phrack.

225. Id.
226. ABA Examining Seizure Rules; Bell South Hackers Appeal Sentences, COM. DAILY, Nov. 28, 1990, at 2.
227. Alexander, supra note 224.
228. COM. DAILY, supra note 226.
229. Alexander, supra note 224.
230. COM. DAILY, supra note 226.
233. Id. at 417.
The scheme was initiated by Riggs who gained unlawful access to Bell South’s computer system, located in Atlanta, Georgia. Riggs then downloaded the text file onto his home computer and transferred the data to Neidorf by using an interstate computer data network. Neidorf edited the text file to conceal the fact it was stolen from Bell South and eventually published his edited version of the text file in his Phrack newsletter. He was later arrested with the other members of the “Legion of Doom.” Of the six counts with which the government originally charged Neidorf, two were for violations of the 1986 Act, subsection (a)(6)(a), which prohibits “trafficking in information through which a computer may be accessed without authorization.” Two other counts were under § 1343 and two were under § 2314.

After the indictment, Neidorf filed several pre-trial motions. In United States v. Riggs, District Judge Bua entered a Memorandum Order which ruled on these motions. First, Neidorf asserted that he could not be charged with wire fraud, because the indictment failed to allege a scheme to defraud. The Judge ruled that the indictment charges that both Neidorf and Riggs devised a scheme to defraud, and took action in furtherance of this scheme. One example of this was Neidorf’s editing of the text file when he first received it over the network from Riggs. The motion was denied.

Neidorf also argued that a fiduciary relationship between him and Bell South was necessary in order for him to be charged with wire fraud, since the charge is based on the deprivation of an intangible right: the text file. The judge denied the motion, stating that the text file is valuable and confidential information and is therefore considered tangible “property,” the deprivation of which could form the basis of a wire fraud charge.

Neidorf also made several other motions (some regarding the charges under § 2314 which will be discussed in that section), including the move to strike words in the indictment he deemed prejudicial, such as “hackers,” and various motions for discovery and disclosure. All of his other motions were also dismissed. The charges regarding com-

234. Id.
235. Id.
236. Id.
237. Id. at 418 (quoting 18 U.S.C. § 1030 (1988)).
238. Id.
239. Id. at 414.
240. Id. at 418.
241. Id.
242. Id.
243. Id. at 419.
244. Id.
245. Id. at 419-26.
puter fraud were not dealt with by the judge as the prosecution indicated it was in the process of drafting a superseding indictment which may not contain any charges under the 1986 Act.\textsuperscript{246}

Subsequently, the government did file a superseding indictment which consisted of ten counts against Neidorf who moved to dismiss all of them.\textsuperscript{247} Once again, in \textit{United States v. Riggs},\textsuperscript{248} Judge Bua entered a Memorandum Order to rule on Neidorf’s motion to dismiss the superseding indictment.\textsuperscript{249} The superseding indictment contained no charges under 18 U.S.C. § 1030. All of the charges were under either 18 U.S.C. § 1343 or 18 U.S.C. § 2314.\textsuperscript{250} The superseding indictment now charged that not only did Neidorf and Riggs enter into a scheme to pilfer information from Bell South, but their scheme also included other valuable computer-stored information as well.\textsuperscript{251}

This time, Neidorf challenged the charges on First Amendment grounds,\textsuperscript{252} the fact that some of the charges are unconstitutionally vague as applied to his conduct and that the indictment “fails to allege a

\begin{thebibliography}{9}
\bibitem{246} \textit{Id.} at 416 n.1.
\bibitem{248} \textit{Id.}
\bibitem{249} \textit{Id.}
\bibitem{250} \textit{Id.} at 557-58.
\bibitem{251} \textit{Id.} at 558. The court stated that the objective of the scheme could now be described as follows: “[T]o fraudulently obtain and steal private property in the form of computerized files by gaining unauthorized access to other individuals’ and corporations’ computers, copying the sensitive computerized files in those computers, and then publishing the information from the computerized files in a hacker publication for dissemination to other computer hackers.” \textit{Id.}
\bibitem{252} The First Amendment implications of the entire area of computer crime are now being scrutinized by various groups. There are countless issues involved, and the topic and how it relates to computer crime could probably generate an entire Law Review note on its own.

For instance, in order to combat the growth of computer crimes, the government has started to organize task forces that deal specifically in this area and include members of the U.S. Attorney's Office, the Secret Service and the FBI. There is a newfound aggressiveness on the part of frustrated federal law enforcement officials in dealing with computer crime. \textit{See} Daly & Hoffman, \textit{Wiretap Snares Alleged Hackers}, \textit{Computerworld}, July 13, 1992, at 1.

Many believe that the task forces have gone too far. The federal officers have begun to execute search warrants and seize bulletin boards during searches and retain them even when no charges have been made. \textit{See} Denning, \textit{supra} note 231. Civil rights activists have charged that the Government agents have intimidated some hackers who requested legal counsel and “stampeded over their constitutional rights.” \textit{See} Alexander, \textit{Hacker Raids Stir up Battle Over Constitutional Rights}, \textit{Computerworld}, June 25, 1990, at 1.

Not only has this type of action led to Fourth Amendment questions, but also First Amendment freedom of speech problems. Members of the computer industry claim that these actions infringe on the freedom of the press to publish. They argue that just like a newspaper, a bulletin board operator should have freedom of speech with their electronic publications, but they do not and “have to be very careful what they post on a board.”
scheme to defraud of which these counts could be a part." The court, once again, dismissed all his motions. Regarding Neidorf's argument that the wire fraud statute should not apply, the judge stated that the "plan involved two major steps: (1) stealing the information by gaining unauthorized access to computers; and (2) disseminating the information to others." Therefore, the plan meets the "in furtherance" requirement of the wire fraud statute since it is certainly an "incident to an essential part of the scheme."

The story has quite an ironic ending, however. While Neidorf was unsuccessful in court, the charges were eventually dropped. Four days after his trial, the government dropped all charges against him after discovering that most of the information that was "stolen" from Bell South and published in Neidorf's newsletter (which Bell South claimed at the time to be valued at $79,000), was actually available to the public who could order it directly from Bell South for $13. While Neidorf was vindicated, the price of victory was $100,000 in legal fees.

They say that there is a "double standard... about what you can say in print or in public and what you can do on a bulletin board." See Sulski, supra note 223.

There are many issues of privacy involved as well. The Justice Department has recently requested a law be introduced in Congress that would require telephone companies to enable their systems to facilitate wiretaps. Mitchell Kapor, the creator of Lotus 1-2-3 remarked: "I find this extraordinarily frightening. Are we living in the kind of adversarial society in which good ends are supported by incredibly pathological means?" See Ratcliffe, Wiretap Plan Draws Conference Fire, MACWEEK, Mar. 23, 1992, at 4.

Those who disagree with how the government is now fighting computer crime are fighting back. Mitch Kapor has formed an official computer hacker defense team which consists of members of two law firms. Alexander, supra. Noted constitutional scholar and Harvard law professor, Laurence Tribe, believes that current constitutional amendments do not protect the rights of the computer user like they should. He has proposed a new amendment to protect privacy in this area. His proposal reads, in full: "This Constitution's protections for the freedoms of speech, press, petition and assembly, and its protection against unreasonable searches and seizures and the deprivation of life, liberty or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted or controlled." Tribe believes this amendment would do for technology what the Ninth Amendment "was meant to do for text." See Resnick, The Outer Limits, NAT'L L.J., Sept. 16, 1991, at 1.

Like most constitutional law issues, these will most likely never be definitively solved. However, being that this whole area of law is so new, the potential for new laws being enacted is high, albeit probably not high enough to warrant a new amendment to the Constitution.

254. Id. at 562.
255. Id.
256. Daly & Hoffman, Wiretap Snares Alleged Hackers; FBI say Hacking no Joke; Notes Theft of Credit Reports, Database Invasions, COMPUTERWORLD, July 13, 1992, at 1.
257. Id.
While the Neidorf saga leaves the law in the area of computer crime muddled and open for a debate of a multitude of issues, what is most interesting about this case is that it occurred in 1990 (long after the 1986 Act was enacted) and it involved a crime performed by hackers belonging to a computer “club.” The computer was their way of life and the major focal point of the crime. In the other cases mentioned under this section, while a computer was used in some fashion, it was more incidental to the crime. The criminals were not computer wizards, freaks, or cyberpunks. Additionally, they were all prosecuted prior to the 1984 and 1986 Acts.

These distinctions cannot be emphasized enough, because they illustrate the inherent weaknesses of the computer fraud statute. If as in Riggs, the government does not even feel comfortable charging the two offenders with even one count of computer fraud, despite the fact this would seem to be a case tailored to the very purpose of that statute, one has to wonder if the statute is totally useless. So, while Morris was quite encouraging to those who believed the 1986 Act could serve its intended purpose of prosecuting serious computer fraud, this case has to leave people wondering why the government would need to utilize a wire fraud statute and a stolen property act to prosecute what was clearly a computer crime. Perhaps Riggs, Grant and Darden would have fared better had they not pleaded guilty, and instead, went to trial. The prosecution may have been reluctant to use the computer fraud statute against them as well, had the case ever made it to trial.

E. SECTION 1346

This section was enacted to ensure that a scheme to defraud includes depriving “another of the intangible right of honest services.” It must be proven that the scheme was devised with the intent to defraud, which is not easy to prove by incontrovertible evidence; however, this section may have been used to cover the INTERNET Robert Morris worm.

F. SECTION 1362

This statute covers anyone who “maliciously injures or destroys any property . . . or other means of communication, operated or controlled by the United States . . . or use of any such line, or system . . . or delays the transmission of any communication over any such line, or system.

---

258. Branscomb, supra note 79, at 29. A term which is now used to describe “computer skilled, but anti-social individuals who deliberately disrupt computer systems merely for the joy and personal satisfaction which comes from such achievement.”
259. Id. at 47 (quoting 18 U.S.C. § 1346 (West Supp. 1989)).
260. Id.
Since the computer can certainly be operated over any telephone line, this statute could certainly be used if there were malicious intent.

G. SECTION 2314

In *United States v. Jones*, the defendant was charged with five counts under 18 U.S.C. § 2314 of transporting in interstate commerce stolen checks. In *Jones*, the defendant altered accounts payable data and then entered this data into a computer facility, thereby issuing five checks to herself which should have been issued to the company for which she worked. The checks were transported from Maryland to Canada. The defendant argued that the checks were actually forgeries and therefore did not fall within the scope of the statute. The Fourth Circuit Court of Appeals, reversing the decision of the District Court to dismiss the indictment, disagreed and ruled that the checks did constitute stolen property and did not fall under the exclusion of forgeries.

As stated in the discussion of Section 1343, the Riggs case also had charges under this statute. As the court pointed out, this case represented the first time that a court held that the “electronic transfer of confidential, proprietary business information from one computer to another across state lines constitutes a violation of § 2314.” This particular ruling could have a major impact in the handling of future computer fraud cases and is another demonstration (like the wire fraud statute) of a different criminal statute being as or more effective in combatting computer crime.

The question was whether the “proprietary information” contained in Bell South’s text file which Neidorf and Riggs stole constituted a “good, ware, or merchandise” within the scope of the statute. The court ruled that it was and likened the stored information Neidorf had on his computer to any floppy disk which could have been transferred

263. Id.
264. Id. at 353.
265. Id.
266. Id. at 356. The statute provides that “[w]hoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud . . .” 18 U.S.C. § 2314 (1988).
267. Id.
268. Riggs, 739 F. Supp. 414. For a full discussion of the facts and issues relating to this case, see supra notes 223-258 and accompanying text.
269. Id. at 419.
270. Id. at 420.
over state lines.\textsuperscript{271} “In either case, the information is in transferrable, accessible, [and] even salable form,” and would thus be considered goods, wares or merchandise under the statute.\textsuperscript{272} In ruling on the other motions Neidorf makes regarding this statute, the judge held that the computer-stored information did meet the requirement of tangibility,\textsuperscript{273} that Neidorf executed the transfer of the information knowing it was “stolen, controverted or taken by fraud,”\textsuperscript{274} and that § 2314 does not preclude “the application of other criminal statutes to computer-related conduct.”\textsuperscript{275}

All in all, the traditional criminal federal statutes most frequently applied in prosecuting computer related crimes are the mail fraud statute, the wire fraud statute, the transportation of stolen property statute, and the theft and related offenses statute.\textsuperscript{276}

V. “MOD”

On July 8, 1992 a group of five hackers were indicted by a federal grand jury in Manhattan on charges of computer tampering, computer fraud, wire fraud, illegal wiretapping, and conspiracy.\textsuperscript{277} The five defendants, aged 18-22, were part of a group called “Mod,” which stood for “Masters of Disaster” and “Masters of Deception,” among other things.\textsuperscript{278} The indictment charged that the “defendants broke into computers ‘to enhance their image and prestige among other computer hackers; to harass and intimidate rival hackers and other people they did not like; to obtain telephone, credit, information and other services without paying for them; and to obtain passwords, account numbers and other things of value which they could sell to others.’”\textsuperscript{279}

This case is a perfect example of how the government could use multiple statutes to prosecute computer crime. In this case, the five defendants were accused of engaging in a widespread pattern of computer crime.\textsuperscript{280} The indictment alleged that the “defendants broke into telephone switching computers operated by Southwestern Bell, New York Telephone, Pacific Bell, U.S. West and Martin Marietta Electronics In-

\textsuperscript{271} Id. at 421.
\textsuperscript{272} Id.
\textsuperscript{273} Id. at 422.
\textsuperscript{274} Id.
\textsuperscript{275} Id. at 423.
\textsuperscript{276} Tramontana, supra note 92, at 263.
\textsuperscript{278} Id.
\textsuperscript{279} Id.
\textsuperscript{280} Ramirez, 5 Are Indicted in Computer Credit Theft, N.Y. TIMES, July 9, 1992, at 14.
formation and Missile Group.\textsuperscript{281} Southwestern Bell reported losses of $370,000 as a result of having to reprogram its computers.\textsuperscript{282}

The charges also alleged that the defendants broke into a Tymnet data network in order to intercept communications being transmitted through the network, and gained access to TRW, a credit agency, thereby gaining access to credit reports, telephone numbers and other related information on various individuals.\textsuperscript{283}

In addition, the indictment alleged that the defendants sold information on how to access credit services and almost wiped out all the information contained within the Learning Link computer operated by Channel 13 in New York City.\textsuperscript{284} Notably, this was the first federal investigation to engage in court-authorized wiretapping in order to obtain conversations and data transmissions between computer hackers.\textsuperscript{285}

Out of an 11-count indictment, only one was for a violation of the 1986 Act. The defendants were charged with one count of unauthorized access of computers under 18 U.S.C. § 1030(a)(5)(a).\textsuperscript{286} The other ten counts were for violations of various statutes, including wire fraud (section 1343) and possession of unauthorized access devices (section 1029).

All five defendants have pleaded not guilty to all charges. Craig Neidorf’s case may have an effect on how this case is handled by the defense and prosecution. The prosecution may have an uphill battle in

\textsuperscript{281} Supra note 277.

\textsuperscript{282} Id.

\textsuperscript{283} Id. at 3.

\textsuperscript{284} Id. at 4. According to the indictment, "the information on the Learning Link was destroyed and a message was left on the computer that said: ‘Happy Thanksgiving you turkeys, from all of us at MOD.'" Id. at 4-5.

\textsuperscript{285} Id. at 5. The defense will most likely argue privacy and other constitutional issues at trial due to the use of wiretaps in this case.

\textsuperscript{286} Id. at 19. The only Grand Jury charge under section 1030 was as follows:

Between on or about January 1, 1991 and on or about January 1, 1992, in the Southern District of New York and elsewhere, JULIO FERNANDEZ, a/k/a ‘Outlaw,' JOHN LEE, a/k/a/ ‘John Farrington,' a/k/a/ ‘Corrupt,' and MARK ABENE, a/k/a ‘Phiber Optik,' the defendants, and others whom they aided and abetted, unlawfully, willfully, knowingly and intentionally did access federal interest computers without authorization, and by means of such conduct did alter, damage and destroy information in such federal interest computers and prevent authorized use of such computers and information and thereby cause loss to one or more others of a value aggregating $1,000 and more during a one year period, to wit, JULIO FERNANDEZ, JOHN LEE, MARK ABENE, and others whom they aided and abetted, accessed Southwestern Bell computers without authorization and by means of such conduct altered calling features, installed back door programs, and made other modifications which caused losses to Southwestern Bell of approximately $370,000 in the form of expenses to locate and replace computer programs and other information that had been modified or otherwise corrupted, expenses to determine the source of the unauthorized intrusions, and expenses for new computers and security devices that were necessary to prevent continued unauthorized access by the defendants and others whom they aided and abetted. Id. at 19.
proving damages to Southwestern Bell in the amount of $370,000, just as in Neidorf's circumstance the prosecution ended up dropping the charges since the damages claimed by Bell South were unfounded. One has to wonder if all five defendants are following Neidorf's example by pleading not guilty to all charges, rather than plea bargaining to a lesser charge like Riggs, who ended up being sentenced to jail as a result. In any event, if the charge under the 1986 Act ends up being dropped like it was in Neidorf's case, the questions regarding the effectiveness of the 1986 Act in cases such as this will increase and the outcry for an amendment to the 1986 Act will continue.

VI. VIRUSES AND AMENDMENTS

As stated at the inception of this article, computer viruses such as Michelangelo are being recognized as the major threat to computer security. There are currently more than one thousand known computer viruses and new ones are continually surfacing at a rate of approximately six per day.

Computer viruses have been called "rogue programs that transport themselves by becoming secretly attached to programs and data files." First, a virus will insert an executable copy of itself onto another program. Then, because this process only takes a few seconds, the virus can secretly attach more copies of itself onto other programs within its reach without the operator ever knowing. A virus does not serve any beneficial goal and can actually lead to malicious and severe results. In addition, the programmer of the virus does not obtain anything from the computer itself—he or she merely interferes with the others' "use" of the computer system.

Due to the threat of damage a computer virus can enact, many have wondered if the 1986 Act could adequately penalize acts involving computer viruses, especially when the drafters of the 1986 Act could not foresee the advent of computer virus crime. While Morris technically involved a computer "worm," his bug was quite similar to a virus and illustrated the extent of damage a virus could do. And, while Morris was convicted under the 1986 Act, many believe the 1986 Act is still

289. Markhoff, supra note 287.
290. Tramontana, supra note 92, at 255.
291. Id. at 260.
292. Id. at 262.
293. Id. at 266.
294. See supra notes 121-71 and accompanying text.
not sufficient in dealing with computer virus crime. For instance, Kenneth Walton, deputy chief of the FBI's criminal investigation division, has said that the 1986 statute is limited because it requires the authorities to prove both criminal intent and damage, which to Walton are "two swing points that make investigations very difficult." The Director of the FBI, William Sessions, has stated that: "Existing criminal statutes are not specific on the question of whether unauthorized access is a crime where no theft or damage occurs, and there is no statute specifically addressing viruses."

In recognition of the limitations of the 1986 Act in this area, on January 3, 1989, Representative Wally Herger introduced the Computer Virus Eradication Act of 1989 [hereinafter the Virus Bill]. The Virus Bill sought to amend 18 U.S.C. § 1030 by adding a new section that would specifically deal with computer viruses. Representative Herger commented that "[a]lthough the '86 statute covers most forms of computer crime, viruses which are designed by individuals with 'authorized' access to computer systems, or viruses that are not designed to delete files, may not fall within the limits of the Act. Our bill addresses these problems. It would close these loopholes . . . ."

The new section would penalize any individual who "knowingly inserts into a program for a computer, or a computer itself, information or commands, knowing or having reason to believe that such information or commands may cause loss . . . to users of such [a] computer. . . ." A key to this new provision is that it contains a scienter requirement of "knowing" rather than "intentional." Previously, when Congress passed the 1986 Act, it changed the scienter requirement of section 1030(a)(5) from "knowing" to "intentional" in order to prevent careless conduct from being a crime. With this new amendment, such careless conduct could now become a crime. For instance, a hacker could create a virus for his or her own use and carelessly transmit it to another computer via an electronic mail transmission. Even though there was no intent to transmit the virus, the scienter requirement of the Vi-

300. Id.
301. H.R. 55, supra note 297.
303. Id. at 1174.
ruses. Bill could be satisfied simply by the fact the hacker knew of the potential harm the virus could cause.\textsuperscript{304}

The Virus Bill also included a provision which allowed for a civil action.\textsuperscript{305} This section provided that “[w]hoever suffers loss by reason of a violation of subsection (a)(7) may, in a civil action against the violator, obtain appropriate relief. In a civil action under this subsection, the court may award to a prevailing party a reasonable attorney's fee and other litigation expenses.”\textsuperscript{306} Under this provision, the victims of the INTERNET virus might have been able to recover all costs incurred in eliminating the virus and restoring computer systems.\textsuperscript{307} While the Virus Bill was believed by many to be a definite improvement over the 1986 Act in deterring computer viruses,\textsuperscript{308} it never actually came up for a vote in either the House or Senate in the first session of the 101st Congress, and therefore was never passed.\textsuperscript{309}

Another bill submitted to the House of Representatives in 1989 was entitled The Computer Protection Act of 1989 (the Protection Act), and was introduced by Representative Tom McMillen.\textsuperscript{310} The bill did not amend 18 U.S.C. § 1030. Rather, it sought to amend 18 U.S.C. § 1368, the malicious mischief and sabotage code.\textsuperscript{311} The Protection Act proposed that willful and knowing sabotage “of a computer hardware system and the associated software . . .” would be a felony.\textsuperscript{312} It also provided for civil remedies similar to the Virus Bill.\textsuperscript{313} However, the bill has been criticized in that it does not define what constitutes “sabotage,”\textsuperscript{314} and its wording is unconstitutionally vague\textsuperscript{315} and ambiguous.\textsuperscript{316} Like the Virus Bill, this bill also never passed.

On June 18, 1991 Senator Patrick J. Leahy introduced a new bill entitled The Computer Abuse Amendments Act of 1991 (Abuse Act).\textsuperscript{317} The Abuse Act sought to amend section 1030(a)(5) of the 1986 Act.\textsuperscript{318} It
was specifically created to deal with viruses and worms.\textsuperscript{319} The Abuse Act would make it a felony to knowingly transmit a disruptive program with the intent to damage the system or information within the affected computer or to deny the use of the system, if the transmission: (1) occurred without authorization of the people responsible for receiving the transmission; and (2) caused loss or damage of greater than one thousand dollars during any one year period.\textsuperscript{320} The Abuse Act also creates a misdemeanor for recklessly transmitting a destructive computer or code.\textsuperscript{321} The Abuse Act would also expand the coverage of 18 U.S.C. § 1030 to include a computer used in interstate commerce, as opposed to only “federal interest” computers.\textsuperscript{322} Finally, the Abuse Act also makes civil remedies available, such as compensatory damages, injunctive relief and other equitable relief.\textsuperscript{323}

The sponsor of the bill, Senator Leahy, stated that in drafting the legislation he sought to balance the punishment with the need to encourage legitimate experimentation.\textsuperscript{324} Hence, while it is a felony to intentionally cause harm to a computer, the Abuse Act recognizes that some computer incidents are not malicious or intentional. These acts, such as “knowingly” transmitting a computer program with “reckless” disregard, are treated as misdemeanors.\textsuperscript{325} A cosponsor of the Abuse Act, Senator Herb Kohl, also emphasized the balancing act the new legislation sought to impose: “This amendment recognizes the difference between malicious, intentional behavior, and unintentional, accidental incident. As a result, the proposed language treats these different degrees of intent in a legally appropriate manner. If the harm was intended, or the virus was knowingly transmitted or transmitted with reckless disregard of a substantial and unjustifiable risk, the act is punishable as a criminal violation and a civil cause of action arises. If, on the other hand, there was an honest mistake, there is no violation or cause of action.”\textsuperscript{326}

The Abuse Act contains much broader language than the 1986 Act and was drafted to specifically deal with the problem of computer viruses. The fact is, however, that if the Abuse Act were enacted prior to \textit{Morris}, that case may not have had the same result. In fact, the Abuse Act would essentially overrule \textit{Morris} since it requires the transmitter

\begin{thebibliography}{9}
\bibitem{320} S. 1322, § 1030(a)(5)(A)(i).
\bibitem{321} \textit{Id.} § 1030(a)(5)(B)(i).
\bibitem{322} \textit{Id.}
\bibitem{323} \textit{Id.} § 1030(c).
\bibitem{324} Leahy Statement, \textit{supra} note 319, at S8031.
\bibitem{325} \textit{Id.}
\end{thebibliography}
of a program to intend that the transmission cause damage, while in *Morris* the evidence demonstrated that the defendant did not have intent to cause harm or damage (emphasis added). 327 Therefore, the 1986 Act would prove stronger in combating computer viruses than the Abuse Act in that one instance. Perhaps that is why the Abuse Act has failed to gain congressional approval and is still pending. 328 Even though the bill was combined with the omnibus crime bill in November 1991, it still could not get through the Senate. Therefore, the 1986 Act remains untouched at the present time.

VII. CONCLUSION

Today, it is commonplace to see a computer in the home as well as the office. The use of computers will significantly increase in the future as the prices on hardware and software decrease and the demand for computer-literate employees soars. With the additional use of computers will come additional problems similar to the ones discussed in the above cases. With this in mind, it is imperative that Congress devise an effective scheme that will not only protect corporations, but will also protect personal computer users from hackers and their viruses.

As my previous discussion indicates, computer viruses and similar disruptive programs have been identified as the major threat to the security of computer programs and databases in the United States. They should be, and are, the primary concern of businesses, law enforcement agencies and any other individual dealing with computer crime throughout the nation. There are many who believe that the 1986 Act, in its current form, is not adequate to deal with this problem, which has led to the call for amendments to the 1986 Act. However, while two amendments which deal specifically with the problem of viruses have been proposed, neither one has been enacted.

The reluctance of Congress to amend the 1986 Act in any way is most likely due to several factors. First, the *Morris* case proved that a successful prosecution under the 1986 Act for the insertion of a computer virus into a computer network was possible. Even though the 1986 Act was written prior to the advent of computer viruses, the fact that Morris was satisfactorily prosecuted under it showed that it has potential in this area.

Second, as Senator Leahy has indicated, there is a definite need for those few who experiment on computers and subsequently uncover problems with programs and discover better ways to perform various

327. Lyman, supra note 291, at 1174 n.44.
computer functions. In fact, it is generally these type of individuals who end up inventing new programs. So, we have to balance the need for these individuals to use computers and run the risk of somehow causing damage to another computer by mistake against the potential for hackers disrupting countless networks and possibly creating viruses such as Michelangelo, which can cause the nation severe damage.

Third, Congress may possibly recognize that by broadening the language of the statute, it may raise many constitutional issues. For instance, if the Virus Bill or the Abuse Act were passed, one could foresee where the Justice Department and other federal law enforcement agencies might begin to use wiretaps (as they did in the "Mod" case) and other electronic surveillance instruments on a widespread basis. This, of course, would lead to First Amendment privacy issues.

The question is, how far does one go to protect against computer crime? I assert that we need to go a lot further than the government has gone to protect against computer crime. Computer crime has cost this country millions of dollars. The potential for damage to defense systems and other related databases is enormous. The laws we currently have in effect to combat computer crime are barely adequate.

The major consideration Congress should have in enacting any law combatting computer crime should be its deterrent value. I contend that when you have a federal law in action for over seven years, and only one case is prosecuted under that law, it has no deterrent value whatsoever. There is no hint of the Act's deterrent value from hackers who have been prosecuted in the past.

This is precisely why a new computer crime law is essential at this time. While I am not convinced that any of the proposed amendments adequately include what desperately needs to be covered, I do believe a change needs to be implemented. I would propose a slightly different approach to tackling the problem.

It is apparent from the cases that the Justice Department does not feel confident using this statute to prosecute perpetrators of computer crimes. Why not? Why is it able to utilize other crimes such as wire fraud and mail fraud in the prosecution of computer-related cases without any effort, yet is unable to apply the actual statute that was designed to be used in cases such as this?

This is where Congress should look first—to the various statutes that have been successful in prosecuting computer crime. What is it about wire fraud that enables a prosecutor to apply it to almost every computer crime case? Could Congress use some of the wording of the wire fraud statute in a new amendment to the 1986 Act? Why not? Why not encompass part of the mail fraud statute as well into the 1986 Act? I believe any individual would be deterred more by one law that is
consistently used in every case than by having ten counts of different crimes charged and knowing that nine of them will be thrown out anyway before going to trial. I would rather have ten counts of computer fraud in a computer crime case than two counts of computer fraud, two counts of wire fraud, two counts of mail fraud, etc.

Therefore, I propose that Congress amend the 1986 Act, making it strong enough that the need to have numerous counts of other criminal charges will not be required in every case. I am not by any means suggesting that a prosecutor should not look to all statutes available; I am simply contending that the deterrent value of a computer crime law would be much higher if there were more Morris cases, where a computer crime was successfully prosecuted under a computer fraud statute. This would be accomplished by rewording the statute to overlap in areas where other statutes have been successful in prosecuting computer crimes.

I also believe there are still a lot of prosecutors who are wary of learning and feeling comfortable with this law, since it is so technical and they may know little or nothing about computers in the first place. The legislative history of the 1986 Act indicates that Congress heard many speakers from the Justice Department elaborate on what type of law was needed to prosecute computer crimes. I believe that the Justice Department itself was unclear in 1986 on how to prosecute these crimes and now, six years later, it has a much higher comprehension of the weaknesses and strengths of the 1986 Act. Therefore, I would also recommend that the Justice Department institute immediate training within its ranks on how to prosecute computer crime under this statute. A team of experts within the department, those who have been involved in computer crime prosecutions, should go from office to office as they did with the RICO statute and give examples of how and when this statute should be used. The only way you are going to have deterrence is if actual convictions under this law are made.

Computer crime is here to stay. However, the usual perpetrators of the more serious computer crimes are generally younger and therefore more easily influenced. If there were more prosecutions under a computer statute, I believe that deterrence would work and we may see a decrease in this type of crime. In addition, it is essential that the Justice Department become more familiar with computers and the laws that protect them.

Finally, it should be mentioned that there is no simple answer to this problem; the fact that Congress has not acted on two proposed amendments is proof enough of that. However, when other statutes are used more often to prosecute computer crime than the statute specifically entitled “The Computer Fraud and Abuse Act,” there is a serious
problem that needs to be addressed. In this case, there is a statute that requires an amendment.