Volume 93
Issue 3 *Dickinson Law Review - Volume 93, 1988-1989*

3-1-1989

Computer Viruses and the Law

Camille Cardoni Marion

NOTABLE STUDENT WORK

Computer Viruses and the Law

I. Introduction

On November 3, 1988, a computer virus spread across the nation in what experts called the largest virus outbreak thus far in the nation.[1] The virus spread rapidly throughout a nationwide network of computers which included Arapnet, a Department of Defense computer network. This well-publicized event illustrated the vulnerability of a sophisticated government computer system and raised new and far-reaching legal questions regarding the security of all computer systems and networks.

The network that fell victim to this virus is known as Internet, a computerized information system used by universities, military contractors, research centers, and the Pentagon. Internet links approximately 50,000 computer terminals across an intricate electronic network. During the day-long epidemic, the virus spread throughout the network to wherever local computers and systems were linked. The systems that were connected to the network soon filled up with extraneous computer information, which caused the computers to perform extra calculations and in some instances to overload and shut down.[2]

The ill-fated virus program that wreaked this havoc was allegedly developed by a computer science graduate student. The program was part of a personal experiment that he began after discovering a flaw in security that allowed him to access the restricted Arapnet network.[3] The student's original intent was purportedly to spread a "harmless" virus program secretly through the nationwide system. The program was to spread slowly from computer to computer throughout the network leaving behind one copy of the illicit program on each machine. The student planned to eventually inform

1. New York Times, Nov. 4, 1988, at A1, col. 3.
2. *Id.*
3. New York Times, Nov. 6, 1988, at 30, col. 2.

users of the intrusion of the virus as a way of pointing out the weaknesses in the system. Due to a single incorrect number written within the computer code of the virus, however, the program copied itself hundreds of times into each machine it contacted.[4]

Although it appears that no data was lost, the research and scientific community temporarily lost the use of the communications network, in addition to tens of thousands of individual computers. Many staff hours were spent checking, purging and restoring operations of the computers on the network.[5] Because of the difficulty in assessing the full and possibly hidden impact of the virus and determining how many individual programs were affected, the amount and extent of physical and financial damages cannot yet be estimated.[6] Some computer experts estimate that clearing the machines of the virus will cost millions of dollars in labor.[7] But as one computer expert stated, "The big issue is that a relatively benign software program can virtually bring our computing community to its knees and keep it there for some time."[8]

Incidents similar to the November 1988 virus have occurred before over the past few years, but none have been of this magnitude or have generated this much publicity. Perhaps the greater publicity associated with this latest incident will awaken the public to the potential for substantial disruption and possible destruction of computer networks essential to defense, public safety, and business. Many viruses detected prior to this outbreak have been relatively minor. The magnitude and speed of this recent virus have highlighted the fragility of existing computer security systems and have raised many questions regarding the ultimate effects such an invasion may produce in the future.[9]

The computer community is split over the gravity of the offense. Even though the damage done by this virus may have been accidental, computer managers were angered by the need to spend days ridding their computers of the program. On the other hand, some computer experts feel that the program may have performed a public service by finally causing the computer community to give increased attention to computer security.[10] Not only have these recent events

4. New York Times, Nov. 6, 1988, at 30, col. 3.
5. *Id.*
6. The Washington Post, Nov. 4, 1988, at A4, col. 1.
7. The Washington Post, Nov. 6, 1988, at A9, col. 1.
8. The New York Times, Nov. 4, 1988, at A1, col. 4 (quoting Chuck Cole, deputy computer security manager at Lawrence Livermore Laboratory in Livermore, Cal.).
9. The Harrisburg Patriot-News, Nov. 6, 1988, at 6, col. 3.
10. New York Times, Nov. 6, 1988 at 30, col. 4.

raised technical questions about how computer viruses occur and how they can be stopped, but the events also have raised new and interesting questions regarding legal safeguards and deterrents that exist to help ward off or respond to similar events.

II. What are Computer Viruses?

Computer viruses are computer instructions or small hidden programs that are inserted into a standard computer program or into a computer's operating system. These instructions may replicate many times during a single program execution, infect every program on a computer disk and be passed on secretly to other computers through modems, floppy discs, or network connections.[11]

A programmer creates a virus by writing a computer code which can attach itself to other programs. Once attached, this code may alter the operations of a program or destroy data kept on a computer disk. A virus can "infect" a computer system as a result of programming or by users running an already infected computer program on the system. Unsuspecting users running virus-infected programs allow the virus to establish itself in a computer system. Once established, the virus can access and modify any file the user is authorized to access.[12] Similar to a biological virus, a computer virus spreads rapidly from a single point of infection. Multiplying in geometrical progression as it works its way through a computer system or network, the computer virus may contaminate all files within a computer system.[13]

A computer virus basically carries a genetic code in machine language. The virus may be benign or malicious. A malicious virus can cripple a network with dead-end tasks, erase files, create false information, and in some cases, destroy equipment.[14]

The virus can spread to other computers through exchange of computer programs, through computer networks, or through electronic bulletin boards. Users of the recipient computer rarely know of the infection because viruses are generally designed to remain dormant for some predetermined time. Using the internal clock calendar of its host, the virus can then activate itself at an appointed time or following a specific event, and then perform its designated

11. LEGISLATIVE BUDGET & FINANCE COMMITTEE, REPORT TO THE PA GENERAL ASSEMBLY OF 1988, at 8 (1988) [hereinafter REPORT TO THE PA GENERAL ASSEMBLY].
12. *Id.* at 12.
13. *Id.*
14. *Id.* at 133.

function.[15]

The viruses that have been reported seem to encompass what were previously known as logic bombs, Trojan Horses, and worms. A logic bomb is a computer program hidden within another problem, and when triggered, is usually highly destructive. If the program is set to go off on a certain date, it also includes a "time bomb."[16] A "worm" is a set of instructions that infiltrate and interfere with the computer's ordinary instructions.[17] Sometimes, a program will be given to a user as something useful or enjoyable, but the program contains malicious instructions. Such programs are known as "Trojan Horses."[18]

Computer manufacturers increasingly promote connectivity or networking to computer users. In order for computers to share information, data generated from one computer must be available to another program on a different computer by modem or direct connection.[19] This gives users the ability to link computers within offices, buildings and across the country.[20] The Apple Computer Company even dubbed 1988 the "Year of Connectivity."[21]

With the increased emphasis on networking and connecting personal computers with mainframes, the ability of computer viruses to spread quickly among users has grown. Often personal computers are shared by many people in one location, making it very difficult to contain a spreading virus or identify its source.[22]

Prior to the November 3, 1988 outbreak, the largest group affected by viruses appeared to be home users, small businesses and people who use public bulletin boards.[23] The incidence of reported computer viruses, however, has increased. Over the last two years, viruses have been found on college campuses, home computers, industry networks and even at NASA.[24]

The first computer viruses were created for legitimate purposes. In the 1970s computer security firms created and used virus programs to trace the evolution of programs being copied illegally.

---

15. Hafner, *Is Your Computer Secure?*, BUSINESS WEEK, Aug. 1, 1988, at 70.
16. REPORT TO THE PA GENERAL ASSEMBLY, *supra* note 11, at 44.
17. Gemignani, *What is Computer Crime, and Why Should We Care?*, 10 U. ARK. LITTLE ROCK L.J. 55, 64 n.39 (1987-88).
18. REPORT TO THE PA GENERAL ASSEMBLY, *supra* note 11, at 12.
19. *Id.* at 12-13.
20. Thornburg, *Computer Viruses Use Networks to Spread the Disease of Distrust*, COMPUTE, July 1988, at 10.
21. Bartman, *MS-DOS/MAC Connectivity*, MAC USER, Sept. 1988, at 106.
22. *Id.* at 106.
23. Thornburg, *supra* note 20, at 10.
24. REPORT TO THE PA GENERAL ASSEMBLY, *supra* note 11, at 10-11.

These viruses were supposed to decrease the "pirating," or illegal copying, of computer software among users.[25] Today, computer viruses are an example of a new form of computer vandalism that can have serious implications for persons and businesses who depend upon computers.[26] Businesses rely on computers to run industrial plants, to control production schedules, to process accounts payable and receivable transactions, and to design products. Service industries such as banks and airlines depend on their computers to carry out essential and often very intricate transactions. Financial institutions transmit close to $1 trillion daily using computer networks.[27] Some state governments rely on computers to distribute unemployment compensation and welfare payments, to register motor vehicles and drivers license records, and to record court and criminal records.[28] The proposed Strategic Defense Initiative depends absolutely on computer software.[29]

III. Controlling Computer Viruses

State and federal lawmakers currently face the question of how to punish perpetrators of computer viruses. They must decide whether a computer virus is a computer-related act that is so dangerous to the public welfare that society should punish those who commit such acts through the criminal justice system.[30] The answer to this complex issue requires a balancing of the seemingly harmless effects of a benign virus against the consequences of a more destructive virus. Lawmakers have found it difficult to draw any clear lines. The potential hazard of viruses to banks, governments, insurance companies, hospitals and other institutions that rely on computers emphasizes the need for comprehensive computer crime legislation at both state and federal levels.

A. State Law

State legislators have begun to evaluate their own efforts against computer crime. Forty-eight states have enacted specific computer crime laws.[31] (See Appendix). The acts forbidden and the

25. Marshall, *The Scourge of Computer Viruses*, SCIENCE, April 8, 1988, at 133.
26. Gemignani, *supra* note 17, at 64.
27. *Id.* at 65.
28. Barbagello, "Maybe Viruses Will Get The Legislature 'in the Mood' ", TRIBUNE REVIEW, Sept. 11, 1988.
29. Marshall, *supra* note 25, at 134.
30. Gemignani, *supra* note 17, at 66.
31. DeWitt, *Invasion of the Data Snatchers*, TIME, Sept. 26, 1988, at 67.

penalties imposed for violations vary widely among the states. Meanwhile, the rapid advancement of computer and communications technologies makes the job of legislating against computer crime very difficult.[32]

Most computer crime statutes were written before the risks of computer viruses became known. None of these statutes mention viruses by name and few clearly address how viruses work.[33] In addition, existing computer laws are adversely affected by three key factors: (1) prevailing legal attitudes toward computer crime; (2) easy access to computer systems; and (3) inconsistent legal penalties for violations of existing laws. For those who create illicit viruses, this situation appears to provide the perfect loophole.[34]

1. Prevalent Legal Attitudes.—Traditionally, the prevalent legal attitude toward computer crime has been one of ambivalence. Police and prosecutors manifest this attitude by a reluctance to pursue the computer criminal. The reasons for the lack of prosecution include: (1) understanding the technology of the crime requires special expertise; (2) preparation of a case against a suspect can be particularly time-consuming and tedious; (3) the "criminals" seem more clever than dangerous; and (4) the victims are more likely to be large businesses or banks than individuals.[35]

Courts have manifested their ambivalence by frequently dismissing computer crime indictments. In some cases, the dismissals occurred because the "criminal" act is outside the statute under which charges were brought. Even in cases where indictments were not dismissed, the sentences imposed in successful prosecutions hardly seem to justify the effort made to prepare the cases.[36]

In addition, computer experts in many businesses are reluctant to speak openly about viruses. This reluctance is motivated by the fear of exposing the vulnerability of computer equipment. Industry leaders do not want to talk publicly about their systems' security for fear of being targeted by computer criminals.[37] These fears, combined with the ambivalent attitudes of the police, prosecutors and

32. *Id.* at 66.
33. *Id.* at 67.
34. *Id.* at 67.
35. Gemegnani, *supra* note 17, at 56.
36. *Id.* at 57. For example, one Indiana State Police sergeant spent hundreds of hours compiling a case against a state employee who had gained unauthorized access to confidential files. The employee eventually was convicted of theft of computer time. Gemegnani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681, 713-15 (1980).
37. Keever, *Electronic Invasion*, The Harrisburg Patriot-News, Sept. 12, 1988, at 1 (Business), col. 3.

courts, have made the task of solving the problems associated with computer viruses a challenge for lawmakers.[38]

2. Access to Computer Systems.—In a precedent-setting case, a Texas jury recently convicted a programmer of infecting a computer program with a destructive virus.[39] The defendant, Donald Burleson, was found guilty of planting a computer virus in his former employer's system, wiping out 168,000 sales commission records. Burleson had been an employee of the USPA and IRA Company, an insurance and brokerage firm. The company found a series of programs built into their computer system. Two days after Burleson was fired, the programs activated and were not discovered until two days later. If the programs had gone undetected, damage to the computer system could have amounted to hundreds of thousands of dollars. Burleson was convicted of harmful access to a computer, a third degree felony.[40]

Texas enacted its computer crimes laws in 1985.[41] Likewise, most states now have computer crime statutes in some form.[42] Often the success or failure of a prosecution may depend on whether the statute defines "access" and, if access is defined, whether it covers the alleged unlawful act. A computer trespass case tried under the Washington statute is illustrative. In *State of Washington v. Olson*,[43] the state Court of Appeals dismissed an action against an officer in the University of Washington Police Department who was accused of computer trespass in the first degree. The defendant in *Olson* had obtained printout information on college students through the University's Communications Center. Although the defendant had not retrieved the information as part of an investigation, he still argued that his conduct did not amount to unauthorized access. The Code under which the defendant was prosecuted provided:

> (1) A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains *access* to a computer system or electronic data base of another; and (a) the access is made with the intent to commit another crime; or (b) the violation involves a computer or data base

38. *Id.* at 1 (Business), col. 2.
39. Baltimore Sun, Sept. 21, 1988.
40. TEX. PENAL CODE ANN. § 33.03 (Vernon 1989). The penalty for harmful access is up to ten years in prison and a $5,000 fine.
41. 1985 TEX. GEN. LAWS ch. 600, § 1.
42. Soma, COMPUTER TECHNOLOGY & THE LAW § 7.11, at 225 (1978).
43. 47 Wash. App. 514, 735 P.2d 1362 (1987).

maintained by a government agency.[44]

The state law defined "access" as to "approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, directly or by electronic means."[45] The court reasoned that the defendant's conduct amounted only to unauthorized use of computer data; whereas, the conduct prohibited by the statute was unauthorized access. The court stated that because permission to access the computer was not conditioned on the use of the data, there were no conditions attached to the defendant's computer access. Therefore, even though departmental policy prohibited certain use of data, it did not withdraw permission to *access* the computer. Since the defendant had authorization at the time the information was withdrawn, the Washington statute, which prohibits only unauthorized access, did not cover the action.[46]

Olson emphasizes the necessity for state legislatures to define both the terms of art used in the computer statute and those utilized by the computer industry. Clear definitions are necessary to obtain uniform judicial interpretation and application of statutes.[47] Many state statutes manifest legislative intent to include theft in their statutes. In order to successfully prosecute those who create computer viruses, however, the statutes must also cover interference with computer programs and data in their definitions of computer crime.[48]

California is recognized as one of the nation's leading states in developing computer technology. This high-tech environment has prompted the California legislature to pass one of the most comprehensive computer crime laws in the country.[49] The California statute expresses the intent to expand the protection of "individuals, businesses and governmental agencies from tampering, interference, damage and unauthorized access to lawfully created computer data and computer systems."[50] Subsection B of the California statute contains definitions of terms of art used in the computer industry. The statute defines "access" as a "means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function re-

44. WASH. REV. CODE ANN. § 9a.52.110 (1988) (emphasis added).
45. *Id.* § 9a.52.010(6).
46. *Olson*, 47 Wash. App. at ____, 735 P.2d at 1364-65.
47. Smith, *Who Is Calling Your Computer Next? Hacker!*, 8 CRIM. JUST. J. 89, 107 (1985).
48. *Id.* at 106.
49. CAL. PENAL CODE § 502 (West Supp. 1988).
50. *Id.*

sources of a computer, computer system or computer network."[51] This new law is still untried by the courts.

The California legislature recognized the need for specific definitions in its computer crime statute. These specific definitions are necessary to combat increasingly complex computer crimes, like computer viruses. States such as Washington,[52] which have computer crime statutes, but have failed to define the terms used, face frustration because perpetrators of computer viruses may find a loophole in their statutes.[53] Legislatures must strive to be specific to avoid forcing courts to define technical terms.

3. Penalties for Computer Crime.—Early attempts to prosecute forms of computer "vandalism" under state theft statutes were not successful. In *Lund v. Commonwealth of Virginia*,[54] the Supreme Court of Virginia struck down a grand larceny conviction based on the unauthorized use of computer services. Under common law, services and labor could not be the subject of theft, since neither could be carried away. Lund, a graduate student, needed to use the school's computer for his research. Lund's instructor failed to secure for Lund an official access required for graduate students, and, Lund admitted accessing the computer by using friends' pass keys. Even if his conviction had been upheld, Lund would not have been required to serve a prison term. Such results tend to discourage prosecutors from pursuing those who are suspected of making unauthorized use of a computer system. The Virginia legislature has since passed a computer crime statute to avoid this type of result in the future.[55]

The problem faced by the Court in *Lund* is similar to the problems that other courts encounter in computer virus cases. In cases when, at first glance, the "interference" seems to do no more than inconvenience legitimate users, the question arises whether perpetrators should face criminal or civil penalties. Minnesota Senator Darril Weigsheid introduced a bill in Minnesota to deal with attempted access to critical computer systems.[56] Weigsheid found support for his position by telling his colleagues about a program that displayed a picture of a Christmas tree on computer users' terminals. The seemingly innocuous program demonstrated the powerful nature

51. *Id.*
52. WASH. REV. CODE ANN. § 9a.52.110 (1988).
53. *See* BENDER, COMPUTER LAW § 4B.15[2] (1983).
54. 217 Va. 688, 232 S.E.2d 745 (1977).
55. Gemignani, *supra* note 17, at 62.
56. Bloombecker, *Cracking Down on Computer Crime*, STATE LEGISLATURES, Aug. 1988, at 13.

of viruses. This particular virus became a computerized chain letter and its users did not know they were involved. The virus program copied itself to the address of each users' electronic mail list and tied up the system. Even though the virus was relatively harmless, it caused operators to shut down the IBM electronic mail system until it was removed. Because of the possibility that such viruses could gain access to and disrupt air traffic control systems or medical information and health care systems, or shut down essential utilities, one of the goals of Senator Weigsheid's bill was to "match the severity of the punishment to the level of harm from the crime."[57]

This question also arises in distinguishing treatment of a "malicious" as opposed to a "benign" virus, and whether these intrusions should be penalized under criminal laws or civil remedies.[58] Often a typical computer vandal may have little money with which to pay a judgment. In such cases civil liability would not be a sufficient deterrent. Additionally, bringing a civil action can be expensive and time consuming for the person affected by the virus. The victim may also have difficulty obtaining the evidence necessary to gain a judgment.[59] While civil actions alone do not seem to answer the computer virus problem, there are also concerns about criminal penalties.

Confusion surrounds how viruses should be addressed under the criminal laws. Introducing any "foreign" code into another's computer system can cause a problem, for even a benign virus can have unintentional but devastating effects.[60] State laws cannot ignore such intrusions, even in cases where the original intent was nothing more than teenage curiosity. Some current state laws could be construed as covering these "damageless intrusions." Often, however, the severity of the penalties destroy any hope of successful prosecution. Few prosecutors are anxious to bring felony charges against teenage hackers with no prior offenses on their records.[61] Nevertheless, states must address deterrence in their statutes even though there is a tendency to ignore behavior that does not cause harm. The behavior is a violation of the law and must be sanctioned.[62]

One option for the states whose laws do not adequately address computer viruses is to follow the example of states like California[63]

57. *Id.*
58. Gemignani, *supra* note 17, at 65.
59. *Id.*
60. *See supra* notes 1-7 and accompanying text.
61. Bloombecker, *supra* note 56, at 13.
62. *See* Smith, *supra* note 47, at 95.
63. CAL. PENAL CODE § 502(e) (West 1988).

and Missouri.[64] Though neither state statute mentions viruses specifically in its statute, both address the problem of so-called damageless intrusions. Whether or not there was a malicious intent, the result of any intrusion is time consuming for data processing departments. In addition to purging the system of the virus, time must also be spent in attempting to protect systems from future invasions. Therefore, both California and Missouri laws allow the victim of the computer access to recover the cost of any expenditure incurred by the owner to verify that a computer system was not damaged by the access.[65] California's Act also contains a provision addressing first offenses of computer trespass. This provision also allows for a maximum fine of $250, provided no injury occurred.[66] Adoption of such a provision in state legislation will encourage those that are victimized by a virus, whether malicious or benign, to take action against the perpetrator. This type of provision could apply to computer viruses if states define "access" carefully in their statutes to cover instances when intrusions alter, destroy or damage the computer system, its programs, or its data and instances when damages are incurred as time and money spent purging a virus from a system.

Even though most states provide for criminal penalties, the states differ greatly in the classification of the computer crime as a felony or misdemeanor and the penalty provisions. The New Jersey statute is unique in that it provides only civil remedies for computer related offenses.[67] The California, Delaware, Connecticut, Illinois and Virginia statutes have provisions for civil remedies as well as criminal remedies.[68] The civil remedies may include the right to bring a damage suit or to seek an injunction as well as an enforcement action.

Concern over the vulnerability of government computer systems to computer viruses prompted the Legislative Budget and Finance Committee of the Pennsylvania General Assembly to undertake a comprehensive study of computer viruses and their impact.[69] The Committee analyzed how computer viruses relate to computer crime and whether viruses would be addressed under Pennsylvania law. Ti-

64. MO. ANN. STAT. § 569.099 (Vernon Supp. 1989).

65. CAL. PENAL CODE § 502(e) (West 1988); MO. ANN. STAT. § 569.099 (Vernon Supp. 1989). *See* Bloombecker, *supra* note 56, at 13 (discussing above statutes).

66. CAL. PENAL CODE § 502(d)(3)(A) (West 1988).

67. N.J. STAT. ANN. §§ 2A:38-A-1 to 2A:38-A5 (West Supp. 1985).

68. CAL. PENAL CODE § 502; DEL. CODE ANN. tit. 11, §§ 931-939, 2738 (Supp. 1984); CONN. GEN. STAT. ANN. §§ 53A-250, -261 (1985); ILL. ANN. STAT. ch. 38, para. 15-1, 16D-1 to -9 (Smith-Hurd Supp. 1988); VA. CODE ANN. §§ 18.2-152.1 to -152.14 (Supp. 1986).

69. REPORT TO THE PA GENERAL ASSEMBLY, *supra* note 11.

tle 18, Section 3933 of the Pennsylvania Consolidated Statutes makes it an offense to access, alter, or destroy a computer network, computer program, computer system, software, data base or any other computer part with the intent to disrupt the normal functioning of an organization.[70] The statute also makes intentional unauthorized access an offense.[71] It has two additional provisions that appear unique to Pennsylvania. One provision makes it a crime to intentionally, knowingly, and without authorization give or publish a password, identification code, personal identification number, or other confidential information about a computer.[72] Another provision makes one who is an accomplice in a computer crime subject to prosecution under the statute.[73]

The Committee reasoned that the introduction of a computer virus, which has the ability to access, alter or destroy, appears to be a computer crime falling within this statute. The committee also noted that a computer virus case has never been brought to trial in Pennsylvania. Even if the statute is interpreted as including computer viruses, the committee concluded that the Pennsylvania statute did not adequately address all areas of computer virus activity.[74] Among the specific weaknesses identified by the study were the statute's failure to specifically define the type of action which could be considered an offense, and the failure to relate the penalty imposed by the statute to the damage suffered.[75]

B. Federal Law

The development of federal computer law has been similar to the development of computer law in the states. Congress recognized the need for a comprehensive federal computer crime law. Congress formed a committee to investigate the growing problems of computer fraud and abuse. The committee found that the use of computers in businesses and homes had grown significantly.[76] The committee also determined that existing criminal laws were insufficient to address the problem of computer crime.[77] In response to the committee's findings, Congress passed the Computer Fraud and Abuse Act of

70. 18 PA. CONS. STAT. § 3933 (Supp. 1988).
71. *Id.* § 3933(2).
72. *Id.* § 3933(3).
73. 18 PA. CONS. STAT. § 306 (1982).
74. REPORT TO THE PA GENERAL ASSEMBLY, *supra* note 11, at 14.
75. *Id.*
76. S. REP. NO. 99-432, 99th Cong., 2d Sess. 4, *reprinted in* 1986 U.S. CODE CONG. & ADMIN. NEWS 2479.
77. *Id.*

1986.[78]

The federal statute is not intended to cover all potential computer crime. The Senate investigating committee recognized that some states lack comprehensive computer crime statutes. The committee noted, however, that the Computer Fraud and Abuse Act was intended "to limit federal jurisdiction to those cases in which there is a compelling federal interest."[79] Included among these cases would be those in which the crime itself is interstate, the computers involved belong to the federal government, or certain financial institutions are involved.

The nationwide virus attack of November 3, 1988, has demonstrated that the creation and spread of a computer virus is not a clear-cut federal offense under the Computer Fraud and Abuse Act. In such cases the FBI, charged with enforcing the Act, must determine whether the virus attack involves a federal crime. To date, there have not been any prosecutions under the Act for computer viruses. Similar to other law enforcement agencies, investigations of computer viruses are a new field for the FBI. Complicated procedures and the technical nature of the virus program make it difficult to pinpoint the actual perpetrator.

The Computer Fraud and Abuse Act has six sections defining proscribed behavior under the Act. Four of the six sections do not seem to apply to most computer viruses. Section 1030(a)(1) prohibits obtaining information that has been protected by an Executive Order or statute.[80] Obtaining access to information contained in financial records of financial institutions or consumer credit agencies is unlawful under section 1030(a)(2).[81] Accessing a federal computer knowingly and with the intent to defraud is proscribed by section 1030(a)(4).[82] Section 1030(a)(6) makes it unlawful to display passwords which would permit unauthorized access to others' computers.[83]

The legislative history notes that two sections of the Act were meant to deal with offenders who are completely outside the government.[84] Section 1030(a)(3) makes it an offense to intentionally gain access to a government computer without authorization and to affect

78. Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified at 18 U.S.C. § 1030 (Supp. V 1987).
79. S. REP. No. 99-432, *supra* note 76, at 2482.
80. 18 U.S.C. § 1030(a)(1) (Supp. V 1987).
81. *Id.* § 1030(a)(2).
82. *Id.* § 1030(a)(4).
83. *Id.* § 1030(a)(6).
84. S. REP. No. 99-432, *supra* note 76, at 2486-87.

the government's use of such a computer.[85] In order to prosecute an offender under this section there must be a showing that there was an intent to cause the disruption, that the entry was unauthorized and that the computers involved were either exclusively for the use of the government or used by or for the government of the United States.

Section 1030(a)(5) was designed to penalize those who intentionally, without authorization, access a government computer and alter, damage or destroy computer data belonging to another.[86] There are two circumstances in which alteration, damage or destruction will be penalized. One instance is when data relating to medical care and treatment is altered, damaged and destroyed. The second instance is when the total loss to the victim or victims is $1,000 or more in any one-year period. The loss is to include actual repairs and any other expenses the victim might sustain, "such as lost computer time and the cost of reprogramming or restoring data to its original condition."[87]

Both sections are aimed at punishing those lacking authorization to access any federal computer. Moreover, both sections require a showing of intent to cause the disruption. The difficulty in meeting these statutory requirements for prosecution was evident in the November 1988 virus outbreak. There is no indication that the student intended to alter, damage or destroy data, so it appears that the student could not be prosecuted under the Computer Fraud and Abuse Act.

IV. Security and Prevention

The increasing number of outbreaks of computer viruses have revealed that current computer crime statutes are largely inadequate to deal with the virus problem. Coping with regular outbreaks of computer crime has created difficulties for those charged with prosecuting and enforcing the laws. The lack of statutory law on specific computer crimes causes many of these crimes to go unprosecuted.[88] In some cases those crimes that are prosecuted go unpunished because of the insufficiency of the old laws.[89] These problems are magnified by the difficulties of investigating computer viruses because of the technical nature of the crime. These viruses also point out the

85. 18 U.S.C. § 1030(a)(3).
86. *Id.* § 1030(a)(5).
87. S. REP. No. 99-432, *supra* note 76, at 2489.
88. Smith, *supra* note 47, at 111.
89. *Id.*

vulnerability of business and government computers to outside attack.

Legislators must act to pass legislation that is specific to deal with computer viruses before they are faced with a devastating attack. While the virus introduced by the Cornell student was more of a nuisance, it should serve as a warning that viruses can potentially be extremely destructive. For this reason state and federal governments must be ready to respond. Legislation alone, however, is not enough to deter one who would infect a computer system with a virus. Government and private industry must take steps to improve computer security. Traditionally, computer security was considered after the purchase of a new system.[90] In light of the recent outbreak of computer viruses, computer security consultants are advising those with computer systems to make security a priority.[91]

The recent publicity surrounding computer viruses has triggered a growth of computer vaccine programs.[92] Some computer specialists, however, warn that the effectiveness of such vaccine programs are limited; therefore, a vaccine program should be part of a more comprehensive computer security plan.[93] The best strategy for government and business to combat viruses and other computer crimes is to develop a comprehensive plan regarding computer security and practices before a problem actually arises. While no system can be totally secure, implementing security measures can decrease the incidence of crimes and save businesses, governments and consumers from more damaging losses.[94]

Computer users should first examine their systems, paying special attention to those parts of the system that operate outside conventional data processing departments, such as personal computers and research computers, to determine who has authorized access to the systems and what programs are authorized for use.[95] Then a plan can be developed to either limit physical access to the main systems or to implement access control software to screen any person attempting to access the computer system.[96] Another method to control computer use is to develop written procedures regarding the use of the system.[97]

---

90. Boston Globe, Dec. 6, 1988, at 24, col. 5.
91. *Id.*
92. Wall St. J., Nov. 7, 1988, at B6, col. 1.
93. Washington Post, Nov. 8, 1988, at 7, col. 5.
94. Smith, *supra* note 47, at 110.
95. Wall St. J., Nov. 7, 1988, B6, col. 4.
96. Smith, *supra* note 47, at 110.
97. *Id.*

To further protect against viruses, comprehensive computer security plans should contain a disaster recovery plan and a plan for systematic backup of data.[98] The costs of recovery from a computer virus could be minimized if computer system users have a plan in place to handle such problems. Following the November 1988 virus attack, research facilities and universities that had disaster plans avoided total shutdown of their computer systems.[99] Steps for recovery from a virus should be included in the disaster plan. A critical feature in any recovery plan for a computer catastrophe caused by virus is good backup files. Any computer user must plan systematic backup of data in order to restore the system.[100]

V. Conclusion

The problem of computer viruses covers a broad spectrum of behaviors, from benign nuisance type intrusions to the more malicious destructive intrusions. Laws with clear civil and criminal penalties are needed to address this broad spectrum of abusive behaviors. Legislation and security programs alone cannot be effective as the only deterrence against would-be computer vandals. Education is essential and must include not only the technical dimensions of the problem, but also a focus on the issue of computer ethics. Additionally, clear organizational policies and training regarding appropriate usage are needed to develop a sense of responsibility and accountability among those who have access to powerful computer networks.

Camille Cardoni Marion

98. REPORT TO THE PA. GENERAL ASSEMBLY, *supra* note 11, at 21.
99. The Harrisburg Patriot News, Nov. 5, 1988, A1, col. 1.
100. REPORT TO PA GENERAL ASSEMBLY, *supra* note 11, at 21.

APPENDIX

Here is a compilation of state laws governing computer viruses.
ALA. CODE §§ 13A-8-100 to -103 (Supp. 1986).
ALASKA STAT. §§ 11.46.200(a)(3), .740, .985, .990(1), (3)-(7) (Supp. 1986).
ARIZ. REV. STAT. ANN. § 13-2301E, 13-2316 (1978 & Supp. 1986).
CAL. PENAL CODE § 502 (West 1988).
COLO. REV. STAT. §§ 18-5.5-101, -102 (1986).
CONN. GEN. STAT. ANN. §§ 53A-250, -261 (1985).
DEL. CODE ANN. tit. 11, §§ 931-939, 2738 (Supp. 1984).
FLA. STAT. ANN. §§ 815.02 to .07 (West Supp. 1986).
GA. CODE ANN. §§ 16-9-90 to -95 (1984).
HAW. REV. STAT. §§ 708-890 to -896 (Supp. 1984).
IDAHO CODE §§ 18-2201 to -2202 (Supp. 1986).
ILL. ANN. STAT. ch. 38, para. 15-1, 16D-1 to -9 (Smith-Hurd Supp. 1988).
IND. CODE ANN. §§ 35-43-1-4, -2-3 (Burns Supp. 1986).
IOWA CODE ANN. § 716A (West Supp. 1986).
KAN. STAT. ANN. § 21-3755 (Supp. 1985).
KY. REV. STAT. ANN. §§ 434.840 to 434.860 (1985).
LA. REV. STAT. ANN. §§ 14:73.1 to 14:73.5 (West 1986).
ME. REV. STAT. ANN. tit. 71-a § 357 (1985).
MD. CODE ANN. § 146 (Supp. 1986).
MASS. GEN. L. ANN. ch. 266, § 30 (1983).
MICH. STAT. ANN. § 28-529 (1987).
MINN. STAT. ANN. §§ 609.87 to 609.89 (West Supp. 1986).
MISS. CODE ANN. §§ 97-45-1 to 97-45-13 (Supp. 1985).
MO. ANN. STAT. §§ 569.093 to 569.099 (Vernon Supp. 1986).
MONT. CODE ANN. § 45.2-101, 45-6-310 to 45-6-311 (1985).
NEB. REV. STAT. §§ 28-1343 to 28-1348 (Supp. 1985).
NEV. REV. STAT. §§ 205.473 to 205.477 (1986).
N.H. REV. STAT. ANN. §§ 638:16 to 638:19 (Supp. 1985).
N.J. STAT. ANN. §§ 2A:38-A-1 to 2A:38-A-5 (West Supp. 1985).
N.M. STAT. ANN. §§ 30-16A-1 to 30-16A-4 (1984).
N.Y. PENAL LAW § 156 (McKinney Supp. 1986).
N.C. GEN. STAT. §§ 14-453 to 14-457 (1981).
N.D. CENT. CODE §§ 12.1-06.1-01(3), 12.1-06.1-08 (1985).
OHIO REV. CODE ANN. §§ 2901.01(J)(1), (2), 2913.01(E),(F), (L)-(Q), 2913.04 (Baldwin 1987).
OKLA. STAT. ANN. tit. 21, §§ 1951-1956 (West Supp. 1985).
OR. REV. STAT. §§ 164.125, 164.345-164.365 (1985).

PA. STAT. ANN. tit. 18 § 3933 (Purdon Supp. 1986).
R.I. GEN. LAWS §§ 11-52-1 to 11-52-5 (1981 & Supp. 1986).
S.C. CODE ANN. §§ 16-16-10 to 16-16-40 (Law. Co-op. 1984).
S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to 43-43B-8 (1983 & Supp. 1984).
TENN. CODE ANN. §§ 39-3-1401 to 39-3-1046 (Supp. 1986).
TEX. PENAL CODE ANN. §§ 33.01 to 33.05 (Vernon Supp. 1986).
UTAH CODE ANN. §§ 76-6702 *et seq.* (1979).
VA. CODE ANN. §§ 18.2-152.1 to 18.2-152.14 (Supp. 1986).
WASH. REV. CODE ANN. §§ 9A.48, 100, 52.110 to 52.130, 56.010 (West 1977 & Supp. 1986).
WIS. STAT. ANN. § 943.70 (West Supp. 1986).
WYO. STAT. §§ 6-3-501 to 6-3-505 (1983 & Supp. 1986).