4-1-1994

Computer Viruses: Legal Aspects

Robert J. Malone

Dr. Reuven R. Levary

COMPUTER VIRUSES: LEGAL ASPECTS

by Robert J. Malone*
Dr. Reuven R. Levary

* Robert J. Malone is a J.D. / M.B.A. candidate at the Saint Louis University Law School and the Saint Louis School of Business Administration. Dr. Reuven R. Levary is Professor of Decision Sciences at Saint Louis University. He received B.S. and M.S. degrees in Electrical Engineering from the Technion, and M.S. and Ph.D. degrees in Operations Research from Case Western Reserve University.

I. INTRODUCTION

As computer technology advances and the price of computers declines, these powerful machines become more commonplace in homes and offices.[1] Computers assume an expanded role in people's lives, and individuals become more dependent on computers to perform diverse functions.[2] As this dependency increases, so does the potential for harm from computer abuse. Regrettably, legislation to control such abuse lags behind the increasing incidence of computer crime.[3]

Additional federal legislation is needed to contain the growth of "computer virus" crime. An insidious category of crime ranging between vandalism and terrorism, computer virus crime involves computer programmers intentionally destroying the host computer or its data with their programs.[4] All states except Vermont have existing statutes to prohibit various computer crimes, some of which extend to computer viruses.[5] However, computer communication and user information needs are not restricted by state lines. Many computers communicate with other computers through networks that span the entire nation and often extend into foreign countries. It is estimated that one in every four personal computers has a modem which allows users to communicate with each other over telephone lines.[6] This capacity for widespread communication mandates federal legislation to prevent computer crime.

This article will identify the various types of rogue computer programs commonly called viruses, analyze the current federal statutes regarding computer crime and review proposed statutes designed to prevent computer virus crime.

---

[1] Anne W. Branscomb, *Rogue Computer Programs And Computer Rogues: Tailoring The Punishment To Fit The Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 1-2 (1990).

[2] *Id.* at 2.

[3] *Id.*

[4] Daniel J. Kluth, *The Computer Virus Threat: A Survey Of Current Criminal Statutes*, 13 HAMLINE L. REV. 297, 298 (1990).

[5] Branscomb, *supra* note 1, at 30.

[6] *Id.* at 2.

II. ROGUE PROGRAMS

Rogue programs are a class of computer programs which harm or disrupt a computer system.[7] Like other computer programs, they are not inherently malicious.[8] All programs consist of a series of instructions for the computer to execute.[9] Accordingly, a computer programmer must specifically design the rogue program to produce harm.[10]

A. *Evolution of Rogue Programs*

From the creation of the first computers until 1983, rogue programs were merely theories or experiments by the scientific community.[11] To apply these theories, experimental games were played out at several computer research centers, such as AT&T's Bell Laboratories and Xerox Corporation research center in Palo Alto, California.[12]

The experimental games evolved into "Core Wars," where scientists would match wits by creating a program designed to replicate itself and consume their opponent's program in a computer's core memory. The self-replicating programs were called "organisms" because of their ability to grow without direction from their creator.[13] The "Core War" battles were waged in controlled environments. Nocturnal battles raged in large, isolated mainframe computers, so the organism program usually did not have the opportunity to affect other computers or programs.[14] The secrets concerning these organism programs became public knowledge in 1983

---

[7] The public and the media commonly use the term "computer virus" to describe any harmful or destructive computer program. *See* Raymond L. Hansen, *The Computer Circus Eradication Act of 1989: The War Against Computer Crime Continues*, 3 SOFTWARE L.J. 717, 721 n. 15 (1990). In this paper, the term "rogue program" will be used to describe this class. "Malicious code" is another term for the class of programs intended to cause damage. *See* PHILIP FITES ET AL., The Computer Virus Crisis 7 (2nd Ed. 1992).

[8] Hansen, *supra* note 7, at 721.

[9] FITES, *supra* note 7, at 40.

[10] A "hacker" is a computer programmer who designs programs or series of instructions to perform disruptive tasks. The term "hacker" previously indicated a talented computer programmer or operator, but presently describes a computer criminal. FITES, supra note 7, at 95.

[11] For a brief history of the development of computer viruses, *see* JOHN MCAFEE & COLIN HAYNES, COMPUTER VIRUSES, WORMS, DATA DIDLERS, KILLER PROGRAMS, AND OTHER THREATS TO YOUR SYSTEM 23-25 (1989).

[12] *Id.* at 25.

[13] *Id.*

[14] *Id.*

when Ken Thompson, the originator of the UNIX operating system, described early virus programs and "Core War" activities in a speech to a computer association.[15] Following Thompson's speech, *Scientific American* published an article regarding the early virus programs, and even offered to send readers additional technical details on how to create computer viruses.[16]

After the days of "Core Wars," several major types of rogue computer programs developed: viruses, worms, bombs, trojan horses, and trap doors. They all perform malicious functions but operate in varying ways.

B. Viruses

Computer virus programs earned their name from an analogy to medical viruses, which are also extremely small, hard to locate, spread disease by attaching to other cells, and multiply while devastating the infected organism.[17] Similar to the original "Core Wars" organism, a computer virus program is a series of instructions that infects other computer programs by amending the original computer program with its own instructions.[18] Computer viruses cannot operate in isolation without a host computer system to execute their instructions.

These viruses possess the capability to attach to other programs, replicate, and damage the host system. To spread, the virus program constantly seeks to infect new host computers and programs.[19] If a non-infected computer disk is inserted into a virus infected computer, the virus attempts to spread its infection by checking the disk for existing copies of itself. If the disk does not already have a copy of the virus, the virus will clone itself by copying its own instructions on the new disk.[20] When the newly infected disk is inserted in a different computer, the virus repeats this replication process and continues to spread. This constant spreading process is often referred to as the replication phase.[21] Computer viruses are

---

15 *Id.* at 26; *See also* FITES, *supra* note 7, at 21.

16 MCAFEE, *supra* note 11, at 26; *See also* FITES, *supra* note 7, at 21.

17 FITES, *supra* note 7, at 28.

18 MCAFEE, *supra* note 11, at 1.

19 *Id.*

20 *Id.*

21 James Tramontana, *Computer Viruses: Is There A Legal "Antibiotic?"*, 16 RUTGERS COMPUTER & TECH. L.J. 253, 255 (1990).

difficult to detect because of the sophisticated methods the viruses use to attach and disguise themselves.[22]

1. CATEGORIES OF VIRUS PROGRAMS

To identify and describe computer virus programs, computer programmers and users classify them into categories. One simple method of categorizing virus programs, consistent with the medical virus analogy, denotes computer viruses as either "benign" or "malignant."[23] Benign viruses do not intend to damage the host computer or its data, but are usually created as pranks to disrupt users by displaying a silly message or image on the screen.[24] Benign viruses can, however, cause considerable harm to the users by consuming valuable computer resources.[25] A malignant virus intends to harm the host computer system by altering, changing, or destroying programs and data.[26]

Another method of categorizing virus programs is by type of resulting disruption. Virus programs can be divided into four classes of disruption: innocuous, humorous, altering, and catastrophic. An innocuous virus is harmless to the computer system, and creates no noticeable disruptions for the user because the virus resides in the computer without conflicting with existing systems or application programs.[27] A humorous virus program usually only displays a message or image on the user's screen as a joke or prank. It does not modify or delete any data in the computer system, but can sometimes erase itself and disappear.[28] Innocuous and humorous types of viruses may be considered benign because the host system is not damaged or deleted.

Altering and catastrophic viruses, however, are malignant. Altering viruses modify data within the system.[29] This dangerous type of virus changes information in spreadsheets, word processing documents and data bases without alerting the user of the subtle alterations. For example, an altering virus might change a spreadsheet or database by transposing num-

---

22 *Id.*

23 Kluth, *supra* note 4, at 300.

24 *Id.*

25 *Id.*

26 *Id.*

27 MCAFEE, *supra* note 1, at 60-61.

28 *Id.* at 61.

29 *Id.*

bers or moving the decimal place to alter the information.[30] The catastrophic viruses are the worst, because they can destroy critical system files. A catastrophic virus could erase all the information in a computer system, preventing the system from operating normally.[31]

The Computer Virus Industry Association (CVIA) also categorizes computer virus programs by identifying the location of the computer system that the virus infects.[32] Programs are divided into three classes by infected areas: boot segment, operating system, and general applications.[33] First, boot segment viruses infect the area of a computer disk, either floppy or fixed, which contains programs that execute start-up procedures of the computer system, such as installing the operating system and preparing the system for operation.[34] The boot segment programs are critical to the normal operation of a computer system because they are the primary instructions executed when a computer is activated.[35] If a virus infects the boot sector, it has total control of the system from the first moment that it is turned on because the virus executes itself when other boot sector programs are executed.[36]

Second, operating system viruses infect the programs that manage the resources for the entire computer system. For example, the computer's operating system controls all inputs and outputs, and execution of application programs.[37] An operating system virus is detrimental because the virus program would have control of the computer system's resources and could cause severe problems by changing the manner that system resources are allocated.[38]

Third, application viruses infect general application programs that perform functions for the user such as word processing or spreadsheets.[39] An application virus is the most difficult to detect because the virus can copy itself into any general application program in a computer system. It can hide in word processing programs, spreadsheet programs, communication

---

30 *Id.*

31 *Id.*

32 Hansen, *supra* note 7, at 723.

33 MCAFEE, *supra* note 11, at 61.

34 *Id.*

35 *Id.* at 68.

36 *Id.* at 69.

37 *Id.* at 63.

38 *Id.* at 70-71.

39 *Id.* at 63.

programs, game programs, or any of the countless other office automation programs.[40] Application viruses can also infect programs designed to detect and destroy computer viruses.[41]

2. EXAMPLE OF A VIRUS:

PAKISTANI BRAIN VIRUS

An excellent example of a computer virus program is the "Pakistani Brain" virus. This highly infectious computer virus has infected the boot segments of IBM personal computers (PCs) and compatible systems around the world since 1986.[42] This computer virus originated in illegal copies of software purchased from the Brain Computer Services store in Lahore, Pakistan. The virus spread on pirated copies of the software around the world, especially to the United States where personal computers are more prevalent.[43]

The Pakistani Brain virus is infectious and difficult to detect because of its elegant design and elaborate self-protection techniques which enable it to remain hidden.[44] The Brain rapidly infects any DOS-formatted floppy disk that it comes in contact with and continues to spread from disk to disk.[45] After the Brain virus activates, it erases all information and programs from the disk, and can also display the message:

> WELCOME TO THE DUNGEON
> c 1986 Basit & Amjad (pvt) Ltd.
> BRAIN COMPUTER SERVICES
> 730 Nizam Block

---

[40] *Id.* at 71.

[41] *Id.*

[42] MCAFEE, supra note 11, at 92; *See also* Hansen, *supra* note 7, at 724.

[43] Two brothers, Amjad Farooq Alvi and Basit Farooq Alvi, created the virus as an anti-piracy warning and revenge after some of their own software was pirated. They then sold illegally copied software, such as Lotus 1-2-3 and Wordstar,and placed their virus on these pirated disks which sold to tourists for less than one percent of the cost of the originals. *Id.* at 92-93. *See also* Hansen, *supra* note 7, at 723 n. 25. The virus was easily traced to the two brothers in Pakistan because they placed their names, address, and phone number in the computer instructions and on the displayed message when the virus activates. In addition, Amjad admitted creating the virus by being quoted as saying "Because you are pirating, . . . you must be punished." Branscomb, *supra* note 1, at 15.

[44] Hansen, *supra* note 7, at 723; *See also* Branscomb, *supra* note 1, at 16.

[45] Hansen, *supra* note 7, at 723 n. 5.

Allama Igbal Town
Lahore, Pakistan
Phone: 430791, 443248, 2800530
Beware Of This VIRUS
Contact Us For Vaccination[46]

Even after infecting an estimated 200,000 computers by 1988, the Pakistani Brain virus created a positive side effect. In 1988, when the Brain was at its peak of infections and publicity, proprietary software sales increased dramatically.[47] Computer users felt that it was better to pay the price for safe proprietary software than become infected with a virus similar to the Pakistani Brain.[48]

C. Worm

A worm program is a rogue computer program with the capability of moving through a computer network or bulletin board service by wiggling from computer to computer.[49] A worm moves through a system or a network of systems altering small bits of data or code whenever it can get access.[50] For example, a worm can be instructed to infiltrate bank computer systems, transfer funds to an illicit account, and then erase itself so the worm is never discovered.[51] It is called a worm because it leaves a trail of altered data in the form of zeroes which resembles a worm track.[52]

Unlike virus programs, worm programs do not contain instructions to replicate itself into other programs.[53] If a worm program were to work through a system and attach itself to another program by duplicating itself,

---

[46] *Id.*; Branscomb, *supra* note 1 at 15. One frustrated victim of the Brain virus was Froma Joselow, a financial reporter for the *Providence Journal* newspaper in Rhode Island. She lost over six months of work after she became trapped in the Pakistani Brain's electronic dungeon and it destroyed her notes and drafts of a future article. *Id.* at 14-15. The Brain not only infected Froma's computer, but also infected over 300 computers of an electronic editing system of the *Providence Journal.* MCAFEE, *supra* note 11, at 94.

[47] MCAFEE, *supra* note 11, at 92-93.

[48] *Id.*

[49] Hansen, *supra* note 7, at 721 n. 18.

[50] FITES, *supra* note 7, at 7.

[51] MCAFEE, *supra* note 11, at 75.

[52] FITES, *supra* note 7, at 7.

[53] MCAFEE, supra note 11, at 75.

it would then be considered a virus because of its capability to self-replicate.[54]

Some worm programs perform constructive functions.[55] For example, authorized programmers may execute a worm program to move through a network of computers in search of potential resources for processing tasks that require an inordinate amount of computer time.[56]

1. EXAMPLES OF WORMS

INTERNET/ARPANET WORM

A famous example of a worm program is the InterNet/Arpanet worm. Robert T. Morris Jr., a 23 year old first-year graduate student in Cornell University's doctoral program in computer science, created and inserted a worm program into the linked InterNet/Arpanet networks.[57] The InterNet and Arpanet networks consist of 1,200 individual networks with a total of 85,000 computers linked together for exchanging scientific information between academic institutions.[58] The U.S. Department of Defense also uses these networks to communicate with researchers concerning technology for potential defense applications.[59]

Morris designed and created the InterNet worm program to spread from one computer across a national network of computers, bypassing all security procedures.[60] He released the worm program to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects.[61] Because it occupied minimal amounts of computer time, and did not interfere with the computer's normal operations, Morris expected that the worm would not draw attention.[62]

On November 2, 1988, Morris inserted the worm program in the InterNet network through a computer at the Massachusetts Institute of

---

[54] FITES, *supra* note 7, at 7.

[55] Kluth, *supra* note 4, at 300.

[56] *Id.*

[57] *United States v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991); *See also* MCAFEE, *supra* note 12, at 5.

[58] MCAFEE, *supra* note 12, at 6.

[59] *Id.* at 5.

[60] *Morris*, 928 F.2d at 505; *See also* MCAFEE, *supra* note 11, at 81.

[61] *Morris*, 928 F.2d at 505; *See also* Branscomb, *supra* note 1, at 7.

[62] *Morris*, 928 F.2d at 505.

Technology (MIT) to disguise the source of the worm program.[63] As the worm program rapidly gained access to computers linked in the network, it consumed the memory capacity of each computer through a slight programming error, by repeatedly replicating itself in the memory of each computer it accessed.[64] Within hours, the virus ran rampant through individual networks infecting over 6,200 computers forcing them to either crash or become "catatonic."[65] System managers completely shut down their computer systems because the worm had clogged the memories of the computers to the point where the computers could not perform routine functions.[66] The worm forced certain networks off the air for as long as five days.[67]

The benign InterNet worm did not destroy hardware or data, but did disrupt normal computer operations at military facilities, government agencies, and universities.[68] It cost over a million hours of direct labor hours and eight million hours in indirect costs.[69] To complicate matters, this was the first virus of this magnitude and many programmers around the country duplicated efforts by designing programs to disinfect their own networks while other programmers worked on similar programs.[70] The total cost has been calculated at over 98 million dollars.[71]

In 1990, a jury convicted Robert T. Morris of violating the Computer Fraud and Abuse Act of 1986 by intentionally accessing a federal interest computer, preventing authorized use of the computers, and causing more

---

[63] *Morris*, 928 F.2d at 506.

[64] *Id. See also* MCAFEE, *supra* note 11, at 81.

[65] MCAFEE, *supra* note 11, at 81; *See also* FITES, *supra* note 7, at 26.

[66] MCAFEE, *supra* note 11, at 81.

[67] *Id.* at 6.

[68] Kluth, *supra* note 4, at 301. Victims of the InterNet/Arpanet worm included important research facilities such as Lawrence Livermore Laboratory, NASA's Ames Research Center, the Naval Ocean Systems Command, the Super Computer Center in San Diego and the Rand Corporation. It also affected many academic institutions such as MIT, the California institute of Technology, Stanford, Berkeley, Boston, Purdue, Wisconsin, Harvard, Minnesota, Cornell, and other universities. MCAFEE, *supra* note 11, at 82.

[69] The direct labor hours incurred recovering from the infection included programmers identifying the virus, disinfecting the networks, and restoring the network to normal operation. The indirect costs included the hours that computers could not link into the network for fear of reinfection and lost access time, or hours that user were unable to access and use the information on the networks. MCAFEE, *supra* note 11 at 6.

[70] *Id.* at 8.

[71] *Id.* at 6.

than $1,000 in damage.[72] "He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision."[73]

IBM CHRISTMAS CARD

The IBM Christmas card is a further example of a computer worm program that caused disruption for thousands of computer users. A West German law student innocently sent a graphic image of a Christmas tree to friends through the European Academic Research Network (EARN), but the worm program sent copies of itself including the graphic image of a Christmas tree to all users in the electronic mail system.[74] The worm escaped from EARN and crossed the Atlantic through communication satellites to infect up to 350,000 IBM computers linked to their internal electronic mail system.[75]

The worm worked its way through the electronic mail networks so quickly and sent so many images to users that IBM was forced to shut down its internal mail system for three days to remove the worm, obviously disrupting the flow of information throughout IBM and thus reducing IBM's productivity.[76]

D. Bomb

A bomb is a rogue computer program that has secret programming instructions which enable it to perform harmful acts at predetermined times.[77] There are two types of bombs: time bombs and logic bombs. A time bomb performs its disruptive act on a specified date or time.[78] Instead of executing on a specified date or time, a logic bomb executes when a predetermined event occurs.[79] Hackers often instruct their virus programs to operate as bombs, triggered either by time or by logic.[80]

---

72 *Morris*, 928 F.2d at 506.

73 *Id.*

74 MCAFEE, *supra* note 11, at 99.

75 MCAFEE, *supra* note 11, at 30. *See also* FITES, *supra* note 7, at 23.

76 MCAFEE, *supra* note 11, at 100.

77 Hansen, *supra* note 7, at 723.

78 MCAFEE, *supra* note 11, at 77.

79 *Id.*

80 *Id.*

When a virus program has been instructed to perform a time or logic bomb, it possesses the capability to replicate and spread, and also to attack users with sudden damage.[81]

1. EXAMPLES OF TIME BOMBS

ISRAELI OR FRIDAY THE 13TH VIRUS

The "Friday the 13th" virus program was designed as a weapon of terrorism to infect IBM and compatible personal computers in Israel.[82] This highly infectious virus could replicate into both operating systems and general application programs. It was set to erase all the files within infected computer systems on Friday, May 13, 1988, which was the 40th anniversary of the day Israel became a state.[83] Before the virus could execute on May 13th, the computer staff of Hebrew University discovered the virus through a programming error and avoided the potential disaster by developing programs to identify and disinfect computers that contained the hidden virus.[84] The Friday the 13th virus, as others, continues to be unknowingly distributed and can activate on future occurrences of Friday the 13th.

MACMAG VIRUS

The MacMag or Aldus Peace virus activated on March 2, 1988, the first anniversary of the Mac II introduction, by displaying a universal peace message on Macintosh computers all over the world.[85] The editor of MacMag, Richard Brandow, intentionally infected a publicly used Macintosh personal computer with the virus during a two day conference of Macintosh users.[86] Brandow infected the computer, so it would spread a warning message to users concerning the dangers of software piracy.[87]

---

81 *Id.*

82 MCAFEE, *supra* note 11, at 97; *See also* FITES, *supra* note 7, at 33.

83 MCAFEE, *supra* note 11, at 97; *See also* FITES, *supra* note 7, at 33.

84 MCAFEE, *supra* note 11, at 97.

85 *Id.* at 31. *See also* FITES, *supra* note 7, at 32.

86 Branscomb, *supra* note 1, at 13.

87 MCAFEE, *supra* note 11, at 102.

When the virus activated on its specified date, March 2, 1988, it displayed the message:

> RICHARD BRANDOW, publisher of MacMag, and its entire staff
> would like to take this opportunity to convey their
> UNIVERSAL MESSAGE OF PEACE
> to all Macintosh users around the world

The benign virus displayed the message and an image of a globe before it erased itself without damaging any programs or data.[88]

The virus spread rapidly from users at the conference through bulletin boards and users swapping disks.[89] A consultant to Aldus, a large software publishing house, unwittingly infected his own computer with the virus and then sent an infected disk to Aldus.[90]

The MacMag virus was the first virus program that was unknowingly distributed through proprietary software.[91] It replicated into commercial copies of the Aldus Freehand software, a graphical drawing and painting program.[92] After infecting over 350,000 Macintosh users, the MacMag virus received vast publicity and intangibly affected Aldus' reputation in the software market.[93]

Later, another virus almost made its way into an updated version of the same program, but Aldus detected the virus and contained it before it was distributed in commercial copies of the software.[94]

MICHELANGELO

Michelangelo, a recent virus program, infects the boot sector of computer systems and activates every year on March 6, the birthday of the Renaissance painter and sculptor, by erasing any infected computer's hard disk.[95] Michelangelo furthered the awareness of computer users to protec-

---

88 FITES, *supra* note 7, at 3. *See also* MCAFEE, *supra* note 12, at 102.

89 FITES, *supra* note 7, at 24.

90 MCAFEE, *supra* note 12, at 102.

91 *Id.* at 31.

92 *Id.* at 31.

93 Branscomb, *supra* note 1, at 13; *See also* Kluth, *supra* note 4, at 302.

94 MCAFEE, *supra* note 11, at 31.

95 James Daly, *Michelangelo Virus: Security A Tough Sell*, COMPUTERWORLD, Feb. 22, 1993, at 1.

tion and security through widespread publicity before the virus could attack in 1992.[96]

2. EXAMPLES OF LOGIC BOMBS

SCORES VIRUS

The Scores virus illustrates how a computer virus program could target an individual entity, such as a company.[97] An ex-employee of Electronic Data Systems (EDS), a leading computer consulting and data processing company, created Scores to destroy EDS proprietary programs and data on Macintosh computers.[98] Scores infects general applications programs and activates whenever it identifies a file as EDS proprietary information.[99] After activation, it erases all EDS information.[100]

Since that original Scores virus, other hackers modified the virus to seek and destroy all files, not only EDS files. The modified Scores infected Macintosh computers at NASA, Congressional offices, Boeing Aircraft Company, Ford Aerospace, other government agencies, and thousands of other systems.[101]

LEHIGH VIRUS

The Lehigh virus received its name from Lehigh University where it began infecting a large number of personal computers used by students in 1987.[102] Lehigh spreads by infecting the boot segment of computer disks as they are inserted into infected computers.[103] After it replicates four times, it activates and destroys all the files on the computer's hard disk.[104]

---

96 *Id.*

97 MCAFEE, *supra* note 11, at 103.

98 *Id.*

99 Hansen, *supra* note 7, at 725.

100 *Id.*

101 MCAFEE, *supra* note 11, at 31.

102 *Id.* at 98.

103 Hansen, *supra* note 7, at 724.

104 MCAFEE, *supra* note 11, at 98.

E. Trojan Horse

A Trojan horse is an innocent program that conceals a destructive program such as a virus, worm, or bomb.[105] Trojan horses are a common way for rogue programs to spread from computer to computer.[106]

Hackers often use Trojan horses to seduce users into unknowingly spreading their rogue programs. They often use attractive programs such as games, graphics programs, or pornographic games as Trojan horses which carry the hidden rogue programs.[107] Hackers commonly distribute Trojan horses freely through bulletin board services to spread rapidly.[108] For example, a deceptive hacker may load a chess game program with a concealed virus on a small bulletin board service so whenever a user downloads the free chess game or exchanges the game with another user, the virus spreads.

F. Trap Door

A trap door is an easily accessible method for a user to gain access to a computer system.[109] When a user enters the specified combination of keys, the system allows the user access to files even though the user did not satisfy the normal security procedures.[110] If hackers discover a trap door in a computer system, they can insert rogue programs in that system without the required security authorization.[111]

Programmers usually create trap doors for legitimate purposes. Programmers utilize trap doors as a convenient method of accessing the system to construct, test, and maintain programs, while not affecting any users operating in the system.[112] During construction of the system, pro-

---

105 *Id.* at 76.

106 FITES, *supra* note 7, at 8. The Trojan horse computer program received its name from the large, wooden horse where Greek warriors hid within to gain entry to the besieged city of Troy. Kluth, *supra* note 4, at 298. When the Greeks placed the wooden horse statue outside the gates of Troy, the Trojans assumed the statue was a peace offering and brought the horse into their city. Once inside, the Greek warriors opened the gate to the waiting Greek army and the city of Troy fell. MCAFEE, *supra* note 11, at 76.

107 MCAFEE, *supra* note 11, at 76.

108 *Id.*

109 FITES, *supra* note 7, at 371.

110 *Id.*

111 MCAFEE, *supra* note 12, at 78.

112 *Id.*

grammers create trap doors for convenient access to the system. However, after completion, the trap door is often forgotten and never removed. A trap door is a weak link that can be exploited by a hacker if discovered.

III. FEDERAL PROTECTION

A. Evolution of Computer Crime Legislation

As the number of computers increased, criminal acts where a computer was either the object, the subject, or the instrument of the crime also increased.[113] Prior to 1984, federal prosecutors attempted to apply common law principles to computer crimes.[114] Without concise legislation that defined computer terminology, courts were forced to create analogies between twentieth century computer concepts and traditional common law principles, some dating back to English law.[115]

Common law principles provided an inadequate basis for prosecuting computer criminals because of the specific conduct involved in these crimes.[116] The broad language and inappropriate terminology used in these traditional statutes made prosecution unjustifiably difficult.[117] For example, when prosecuting theft of computer property, the concept of a taking could not address unauthorized access to confidential computer material because no legal precedent existed to determine whether computer information was "property."[118] Further, traditional criminal statutes only applied to computer crime when abusive computer conduct was committed in connection with a traditional crime.[119] Common law principles and traditional criminal statutes did not specifically address computer crime conduct, especially computer virus crime.[120]

In 1984, Congress enacted the first federal computer crime statute, the Counterfeit Access Device and Computer Fraud and Abuse Act.[121] Both

---

[113] Darryl C. Wilson, *Viewing Computer Crime: Where Does The Systems Error Really Exist?*, 11 Computer/L.J. 265, 267 (1991).

[114] *Id.* at 267.

[115] Hansen, *supra* note 7, at 727.

[116] Tramontana, *supra* note 21, at 263.

[117] Hansen, *supra* note 7, at 727.

[118] Wilson, *supra* note 113, at 268.

[119] Tramontana, *supra* note 21, at 264.

[120] *Id.*

[121] Hansen, *supra* note 7, at 730.

the general public and the federal bureaucracy, the largest consumer of computer products and services in the United States, had urged Congress to adopt computer crime legislation for greater protection of computer systems.[122] Congress created the new law to address the unique circumstances and applications of this new form of crime.[123] This computer crime statute had several flaws because it lacked clear definitions of applicable computer terms, clear jurisdictional statements, and incentives for computer crime victims to report the abuse.[124] It was amended two years later.[125]

Currently, there are three components to federal protection against computer crime: the Computer Fraud and Abuse Act of 1986 (CFAA), the Electronic Communications Privacy Act of 1986 (ECPA), and the Computer Security Act of 1987 (CSA).[126] The CFAA is the federal government's "big stick" to wave at potential hackers. The other two acts can be applicable in limited circumstances, but the CFAA is the only weapon in the federal government's limited arsenal.

B. Computer Fraue and Abuse Act of 1986

After enacting their first computer crime statute in 1984 and discovering the flaws in it, Congress quickly amended the Counterfeit Access Device and Computer Fraud and Abuse Act with the Computer Fraud and Abuse Act of 1986).[127] CFAA consists of six primary subsections to prohibit the following conduct:

1) knowing unauthorized access to obtain information that is restricted for national security by Executive Order;[128]
2) intentional unauthorized access to information from a financial institution or consumer reporting agency;[129]

---

122 *Id.* at 728.
123 *Id.* at 727.
124 *Id.* at 729.
125 *Id.*
126 Wilson, *supra* note 113, at 271.
127 Hansen, *supra* note 7, at 731.
128 18 U.S.C. §1030(a)(1) (1990).
129 18 U.S.C. §1030(a)(2) (1990).

3) intentional unauthorized access that interferes with government operation of government computers;[130]
4) knowing unauthorized access to a government computer with the intent to defraud and results in obtaining anything of value other than the use of the computer;[131]
5) intentional unauthorized access to a federal interest computer that results in alteration, damage, or destruction of information in the computer or prevents authorized use of the computer or information;[132] and
6) knowingly trafficking passwords or similar information with the intent to defraud and the trafficking affects interstate or foreign commerce, or a federal interest computer.[133]

Two of the six subsections of the CFAA apply to computer virus crime. First, subsection §1030(a)(3) prohibits intentional unauthorized access that interferes with the federal government's use of a government computer.[134] This subsection applies to a computer virus program, but only if the virus affects the operations of a government computer.[135] Even with this restriction, the subsection still has some utility to federal prosecutors because "the federal government is the largest consumer of computer products and services in the United States."[136] However, this subsection neglects to protect many computer systems and networks in the private sector.[137]

Second, subsection §1030(a)(5) prohibits altering, damaging, or destroying information, or preventing authorized use of a "federal interest computer."[138] These are defined as computers used by or for the U.S. government, or for a financial institution[139] or as one of two or more computers linked in more than one state.[140] By including the latter defi-

---

130 18 U.S.C. §1030(a)(3) (1990).
131 18 U.S.C. §1030(a)(4) (1990).
132 18 U.S.C. §1030(a)(5) (1990).
133 18 U.S.C. §1030(a)(6) (1990).
134 18 U.S.C. §1030(a)(3) (1990).
135 Tramontana, *supra* note 21, at 267.
136 Hansen, *supra* note 7, at 729.
137 Tramontana, *supra* note 21, at 267.
138 18 U.S.C. §1030(a)(5) (1990).
139 18 U.S.C. §1030(e)(2)(A) (1990).
140 18 U.S.C. §1030(e)(2)(B) (1990).

nition, which addresses interstate computer crime, this subsection is substantially broader than the previous applicable subsection which prohibits unauthorized interference with the federal government's use of computers.[141]

Despite improving the statutory language of its predecessor, the CFAA remains a flawed legislative response to the problem of computer crime.[142] Undefined statutory terms cause parties in a dispute to argue over what meaning should apply.[143] Further, current case law does not provide precedent to interpret the meanings of these statutory terms because the federal government has tried only a few cases under the CFAA.[144] Without defined terms or precedent, courts interpret legislative intent to determine meanings for key terms in the statute. Thus, judges, who are inexperienced with computer technology, must interpret the key terms and apply them to the circumstances of the case at hand.[145]

First, the CFAA fails to precisely define the term "access." The issue is what conduct constitutes "access" and whether computer viruses satisfy the meaning of access within the CFAA. The statute proscribes hackers from intentionally accessing a federal interest computer without authorization.[146] However, many viruses infect computers without the hacker actually physically accessing the computer.[147] A virus program could access the computer by replicating and spreading, or an individual unaware of the virus could insert an infected disk in the computer.[148] The federal courts have not decided the definitional issue of "access" because cases prosecuted under the CFAA have involved virus infections where the hacker physically accessed the computer system.

Second, the "knowing" or "intentional" standard of culpability under the CFAA provides an enormous obstacle for federal prosecutors to overcome.[149] In the case of computer virus crime, the subjective intent or mental state of the hacker is the most difficult aspect for the government

---

141 *Id.*

142 Hansen, *supra* note 7, at 732; See also Wilson, *supra* note 113, at 272. .

143 Hansen, *supra* note 7, at 732.

144 *Id.* at 733.

145 *Id.*at 732.

146 18 U.S.C. §1030(a)(5) (1990).

147 Tramontana, *supra* note 21, at 269.

148 *Id.*

149 18 U.S.C. §1030(a) (1990).

to prove.[150] The hackers last intentional act is the release of the virus. After releasing the virus, the hacker has little or no control over who the virus infects or what damage it will cause.[151] The hacker has reason to know that infection would be likely because that is what the virus program is designed to do, but the statute requires a direct intention to infect computers.[152]

Although the federal government must prove beyond a reasonable doubt that a suspected hacker intended to access the federal interest computer, it is not required to prove a hacker intended to damage the system or prevent authorized use of the computer system. In *United States v. Morris*, Robert Morris accessed a network of computers comprised of academic and government users, and inserted a worm program that uncontrollably forced computers to shut down and prevented many authorized users from utilizing the network.[153] As a defense, Morris claimed that he did intend to access the computer, but he did not intend to prevent authorized use of the computer.[154] His worm program had a slight programming error that caused the worm to consume the memory capacity of computers thereby preventing authorized use.[155] The appellate court interpreted the statute to require the "intentional" standard for accessing the computer, but not for damage or prevention of authorized use.[156]

Third, the CFAA fails to provide an incentive for victims of a computer virus to report the crime. Although the Act provides for offenders to receive potentially substantial jail terms, the Act fails to provide financial restitution or civil remedies.[157] The private sector is hesitant to report computer viruses or pursue civil remedies because victims try to avoid publicity of a virus infection that would compromise the company's reputation or reveal possible vulnerabilities.[158] Corporations, especially financial institutions, want their customers to feel that their information is secure.[159] Another reason for not pursuing civil remedies is victims com-

---

150 Hansen, *supra* note 7, at 734.

151 *Id.*

152 Tramontana, *supra* note 21 at 268.

153 *Morris*, 928 F.2d at 506.

154 *Id.* at 508-09.

155 *Id.* at 506.

156 *Id.* at 509.

157 Wilson, *supra* note 113, at 272; *See also* Hansen, *supra* note 7, at 732.

158 Hansen, *supra* note 7, at 732; *See also* FITES, *supra* note 7, at 139.

159 FITES, *supra* note 7, at 139.

monly do not recover much from the hacker.[160] Without adequate incentives for victims to report the virus crime, the federal government can not effectively enforce the statute.

Fourth, the CFAA lacks broad interstate jurisdiction for federal prosecution of computer viruses. Without clear federal jurisdiction, the federal government is not obliged to prosecute and the hacker might escape state prosecution if he or she resides in a state other than that in which the computer crime occurred. The prosecuting state may lack "in personam jurisdiction," the power to render a judgment over the defendant who is a resident of another state.[161] Without sufficient jurisdiction to prosecute virus crimes that cross state lines, the CFAA can not adequately meet the challenges of prosecuting computer virus criminals.

The CFAA does not specifically prohibit computer viruses, but can apply to computer virus by prohibiting unauthorized access to government or federal interest computers which results in damage or prevents authorized use. The Act has several flaws such as undefined technical terms, a high standard of culpability, non-existent incentive for virus victims to report the crime, and inadequate jurisdictional statements. The Act also limits its protection to government or federal interest computers, and fails to protect computer systems in the private sector.[162] The Computer Fraud and Abuse Act has flaws, but represents some progress toward effective computer crime laws.

C. Electronic Communications Privacy Act of 1986

In limited circumstances of intercepting electronic communication, the Electronic Communications Privacy Act of 1986 can be applied to computer virus crime. The ECPA prohibits unauthorized interception of an electronic communication.[163] Three of eleven sections within the ECPA may be used to supplement the CFAA even though the ECPA statute does not state the term "computer" explicitly.[164] The ECPA is applicable to computer communications in office environments such as electronic mail,

---

160 Hansen, *supra* note 7, at 733.

161 *Id.* at 735.

162 *Id.*

163 Wilson, *supra* note 113, at 272-73.

164 *Id.* at 273.

electronic bulletin boards, digital textual information, and videotext.[165] Application of the ECPA to computer communication would prohibit hackers from improperly accessing users' data transmissions.[166]

In its remedy sections, the ECPA provides fairly substantial civil damages to a victim.[167] The victim may bring a civil action against the suspected hacker and may receive the actual damage or up to $100 a day in statutory damages to a limit of $100,000.[168] This Act also provides for punitive damages in appropriate cases, but the statute fails to describe such cases.[169] In the case of a virus intercepting computer communication, the ECPA statute would be preferred by the victim because it offers civil remedies.[170]

D. Computer Security Act of 1987

The final component of federal legislation to prohibit computer crime is the Computer Security Act of 1987. The CSA is an administrative directive designed to improve the security and privacy of sensitive information in federal computer systems.[171] The Act establishes a governmental focal point, the National Bureau of Standards, for developing security standards and guidelines for other government agencies.[172] In addition, the CSA delegated the responsibility for assuring implementation of the established standards to the National Security Agency and the Department of Defense.[173]

The CSA does not have criminal provisions, but does provide for reasonable attorney's fees and contractual remedies in certain automated data processing disputes.[174]

---

165 *Id.*at 273, n.57.
166 18 U.S.C. §2510(14) (1987)
167 18 U.S.C. §2520 (1987).
168 18 U.S.C. §2520 (1987).
169 18 U.S.C. §2520(b)(2) (1987).
170 Wilson, *supra* note 113, at 274.
171 40 U.S.C. §759 (1987).
172 *Id.*
173 Wilson, *supra* note 113, at 275.
174 *Id.*

IV. PROPOSED FEDERAL LEGISLATION

A. *Computer Virus Eradication Act of 1989*

In 1989, Congress attempted to further the prevention of computer viruses by introducing the Computer Virus Eradication Act of 1989 (CVEA) to amend the existing Computer Fraud and Abuse Act. The proposed amendment would add three key components to strengthen the existing statute against computer viruses. First, the CVEA would add a subsection to describe proscribed virus conduct.[175] Second, the proposed Act would add a penalty for creating and distributing a computer virus to the already substantial penalties of the CFAA.[176] Third, the CVEA would create a civil remedy for victims of computer viruses.[177]

The CVEA would proscribe two types of computer virus conduct. First, the Act would prohibit a hacker from inserting a computer virus into a program or computer that will injure users or others who rely on information in the computer.[178] Second, the Act would prohibit the hacker from knowingly distributing the computer virus to people who are unaware of its existence.[179] By prohibiting these two virus activities, the federal government could prosecute hackers for most current types of rogue computer programs: viruses, trojan horses, worms, and bombs.[180] Like its predecessors, the CVEA suffers from vague terms that would be argued over in court and ruled on by judges who lack the technical experience to adequately decide the issue. For example, the CVEA uses the phrase "information or commands" to describe virus-creating conduct. This phrase has a common meaning, but it might also have a technical computer meaning that was intended when the bill was created.[181] Many future prosecutions of hackers who create and distribute viruses could hinge on a judge's interpretation of the phrase "information or commands"

---

[175] H.R. 55, 101st Cong., 1st Sess. at §2(a)(7)(A) (1989).

[176] H.R. 55, 101st Cong., 1st Sess. at §2(b) (1989).

[177] H.R. 55, 101st Cong., 1st Sess. at §2(c) (1989).

[178] H.R. 55, 101st Cong., 1st Sess. at §2(a)(7)(A) (1989).

[179] H.R. 55, 101st Cong., 1st Sess. at §2(a)(7)(B) (1989).

[180] Rogue programs would satisfy the "inserts into a program or computer . . . " language of the Act. The rogue program instructions are designed to cause harm, which would satisfy the "may cause loss, expense, or risk to health or welfare . . . " language of the Act. Hansen, *supra* note 7, at 740-41.

[181] *Id.* at 737.

and how it applies to the circumstances of a malicious virus program. This is only one example of undefined key terms in the CVEA.[182] To avoid misinterpretation, the CVEA should include technical computer definitions for key terms within the Act.

Similar to the CFAA, prosecution under the CVEA would be difficult because the government must prove the required mental state. Under the Model Penal Code, a "knowingly" standard is satisfied if the defendant performs an intentional act knowing in the particular circumstances that the results of his actions are practically certain to occur.[183] CVEA requires prosecutors to prove beyond a reasonable doubt that the virus hacker knew he created a computer virus and also that he knew or should have known the virus would cause harm or loss.[184] This standard will certainly be an issue during any prosecution of a computer virus hacker because the hacker losses control over the virus program before it can do harm.[185]

One minor connecting word in the CVEA could raise a "loophole" problem for federal prosecutors. The language of the proposed statute has an "and" connecting the two prohibited virus offenses.[186] The CVEA would require the government to prove beyond a reasonable doubt that a defendant inserted a virus into a program or computer, "and" knowingly distributed the virus to unsuspecting users.[187] Federal prosecutors face an unjustifiable burden of proving that the suspected hacker both created and distributed the computer virus.[188] There are situations where a hacker has not performed both acts and might go free from prosecution. For example, a hacker creates a computer virus and accidentally transfers the virus to another user. This hacker did not knowingly distribute the computer virus and therefore has not satisfied the second requirement of the Act. Alternatively, a person finds a computer virus and then intentionally distributes the virus to others who are unaware of the danger. This offender could also go free because he did not satisfy the first requirement of creating the computer virus. Prior to adoption of any statute like the CVEA, the legis-

---

182 *Id.*

183 *Id.* at 739 (citing Model Penal Code § 2. 02 General Requirements on Culpability (Official Draft 1985).

184 H.R. 55, 101st Cong., 1st Sess. at §2(a) (1989).

185 Hansen, *supra* note 7, at 740.

186 H.R. 55, 101st Cong., 1st Sess. (1989).

187 Tramontana, *supra* note 21, at 272.

188 *Id.*

lation should be redrafted to close this type of loophole, as it could threaten the future enforcement of computer crime laws.

The CVEA would provide as substantial a penalty for creating and distributing a computer virus as it would for knowingly gaining unauthorized access to information that is restricted for national security by Executive Order.[189] The penalty is a fine, up to ten years imprisonment, or both if it is the hacker's first offense under the CFAA or the CVEA. If the hacker had been previously convicted under the CFAA or the CVEA, the penalty is a fine, up to twenty years imprisonment, or both.[190] The substantial penalties would be properly within the federal scheme of penalties and would arm the government with a new weapon against computer viruses.[191]

The CVEA was an important step by Congress to improve federal computer crime legislation. This Act would have created an incentive for virus victims to report the infections by providing for civil remedies that include appropriate relief, reasonable attorney's fees, and other litigation expenses.[192] With the possibility of recovering damages, more victims of computer viruses might choose to pursue actions against hackers and report virus infections.[193] If more companies would report virus infections, more virus hackers would be prosecuted. A trend of successful virus prosecutions would reduce the number of hackers willing to risk federal prosecution by creating and distributing computer viruses.

The CVEA would have provided the federal government with broad jurisdiction over computer viruses under the U.S. Constitution's Commerce Clause.[194] This broad federal jurisdiction could be invoked whenever a virus affected interstate or foreign commerce, or was furthered by means of interstate or foreign commerce.[195] Conversely, the CFAA only references interstate transactions when passwords are trafficked across state lines.[196] The broader jurisdiction would increase the threat of feder-

---

189 18 U.S.C. §1030(c)(2) (1990). *See also* H.R. 55, 101st Cong., 1st Sess. at §2(b) (1989).

190 18 U.S.C. §1030(c)(2) (1990). *See also* H.R. 55, 101st Cong., 1st Sess. at §2(b) (1989).

191 Hansen, *supra* note 7, at 744.

192 H.R. 55, 101st Cong., 1st Sess. at §2(c) (1989).

193 Hansen, *supra* note 7, at 745.

194 H.R. 55, 101st Cong., 1st Sess. at §2(a) (1989); *See also* U.S. CONST. art. I, §8.

195 H.R. 55, 101st Cong., 1st Sess. at §2(a) (1989).

196 It proscribes rogue programs "if inserting or providing such information or commands effects or is effected or furthered by means of interstate or foreign commerce. 18 U.S.C. §1030(a)(6)(A) (1990).

al prosecution and therefore, reduce the number of hackers creating and distributing malicious computer viruses.

The most recent version of the CVEA was introduced with thirty-two sponsors in January of 1989. The House Judiciary Committee reviewed the CVEA, and the Subcommittee on Criminal Justice conducted hearings in late 1989. Surprisingly, after widespread bipartisan support for the CVEA, it was not enacted.

B. Computer Protection Act of 1989

In 1989, the Computer Protection Act was also introduced to the House of Representatives. This proposed bill would prohibit any person from willfully or knowingly "sabotaging" a computer system, hardware or software.[197] The bill would allow virus victims to receive appropriate compensatory damages in a civil action against the hacker.[198] Civil remedies would provide a desired incentive for victims to report computer virus infections.[199]

However, the bill failed to further define the key term "sabotage."[200] "Sabotage" could include the creation and distribution of computer viruses, but without a definition in the proposed statute, it is too difficult to determine what conduct is proscribed.[201] The Computer Protection Act suffered the same fate as the Computer Virus Eradication Act of 1989 and was not enacted.

V. CONCLUSION

Congress should reintroduce and enact a corrected version of the Computer Virus Eradication Act. Rogue programs evolved rapidly from theories to games, and finally to varieties of malicious programs that cause electronic terrorism. Federal statutes should continue to change and progress toward effective protection of computer systems to keep pace with developments in computer technology and computer abuse. Each adopted computer crime Act has been an improvement from the prior computer

---

197 H.R. 287, 101st Cong., 1st Sess. at §1368(a) (1989).

198 H.R. 287, 101st Cong., 1st Sess. at §1368(b) (1989).

199 Branscomb, *supra* note 1, at 49.

200 Tramontana, *supra* note 21, at 275.

201 *Id.*

crime law. Congress should correct the flaws in the proposed legislation such as undefined key terms, difficult standards of culpability, vague statutory language, and ineffective incentives for victims to report computer virus crime. The revised CVEA could form the foundation for effective computer virus protection.

APPENDIX A

COMPUTER FRAUD AND ABUSE ACT OF 1986

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—
(1) knowingly accesses a computer without authorization or exceeds authorized access, 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, as defined in paragraph y 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;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, 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.);
(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;
(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;
(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or

prevents authorized use of any such computer or information, and thereby—

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1) (A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2) (A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(3) (A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5)

of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "Federal interest computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.
(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

APPENDIX B

101st CONGRESS
1st Session

H.R. 55

To amend section 1030 of title 18, United States Code, to provide penalties for persons interfering with the operations of computers through the use of programs containing hidden commands that can cause harm, and for other purposes.
IN THE HOUSE OF REPRESENTATIVES
January 3, 1989

Mr. Herger (for himself, Mr. Carr, Mr. Frank, Mr. McCurdy, Mr. Hyde, Mr. Spence, Mr. Donald E. Luckens, Mr. Lewis of Georgia, Mr. Emerson, Mr. Lagomarsino, Mr. Dannemeyer, Mr. Rinaldo, Mrs. Meyers of Kansas, Mr. Sawyer, Mr. Marinez, Mr. Stark, Mr. Holloway, Mr. Hansen, Mr. Inhofe, Mr. Houghton, Mr. Frost, Mr. Sikorski, Mr. Foglietta, Mrs. Boxer, Mr. Whittaker, Mr. Owens of New York, Mr. DeFazio, Mr. Boehlert, Mr. Moorhead, Mr. Mfume, Mr. Shaw, Mr. Neal of North Carolina, and Mr. Gunderson) introduced the following bill; which was referred to the Committee on the Judiciary.

A BILL

To amend section 1030 of title 18, United States Code, to provide penalties for person interfering with the operations of computers through the use of programs containing hidden commands that can cause harm, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Virus Eradication Act of 1989".

SEC. 2. AMENDMENTS

(a) PROHIBITION.-Section 1030(a) of title 18, United States Code, is amended-

(1) in paragraph (5), by striking "or" after "individuals;";

(2) in paragraph (6), by inserting "or" after "United States;"; and

(3) by adding after paragraph (6) the following new paragraph:

"(7) knowingly-

"(A) 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, expense, or risk to health or welfare-

"(i) to users of such computer or a computer on which such program is run, or to persons who rely on information processed on such computer;or

"(ii) to users of any other computer or to persons who rely on information processed on any other computer; and

"(B) provides (with knowledge of the existence of such information or commands) such program or such computer to a person in circumstances in which such person does not know of the insertions or its effects; if inserting or providing such information or commands affects, or is effected or furthered by means of, interstate or foreign commerce;".

(b) PENALTY FOR A VIOLATION.-Section 1030(c)(1) of such title is amended by inserting "or (a)(7)" after "(a)(1)" each place it appears.
(c) CIVIL REMEDY.-Section 1030 of such title is amended-
(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and
(2) by adding after subsection (c) the following new subsection:
"(d) Whoever 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."