IT'S VIRUS SEASON AGAIN, HAS YOUR COMPUTER BEEN VACCINATED? A SURVEY OF COMPUTER CRIME LEGISLATION AS A RESPONSE TO MALEVOLENT SOFTWARE

The Supreme Court's refusal to review the conviction of Robert Tappan Morris[1] sent a message of deterrence to would-be authors of malevolent software.[2] Morris' conviction notwithstanding, existing federal[3] and state[4] legislation addressing malevolent software lacks the specificity and authority required to police this type of destructive computer programming.[5] The shortcomings of current legislation can be attributed to three factors: (1) the rapid growth of computer technology during the past ten years;[6] (2) the increasing prevalence of personal computers in the home;[7] and (3) public misperception regarding the creation and transmission of malevolent software.[8]

This Note examines the effectiveness of federal and state legislation at discouraging the creation of malevolent software and punishing those who create it. Part I classifies and explains the various types of existing malevolent software, providing examples of their destructive potential. Part II reviews existing federal and state legislation designed to combat

---

1. United States v. Morris, 928 F.2d 504 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991). *See infra* part III.A.

2. Throughout this Note, the term "malevolent software" will be used to describe any type of trojan horse, logic bomb, worm, computer virus or stealth virus. *See infra* notes 9-13 and accompanying text.

3. *See infra* part II.A.

4. *See infra* part II.B.

5. *See infra* part IV.

6. In 1982, an IBM Personal Computer based on the Intel 8086 processor sold for approximately $5,000. Nick Baran, *Two Worlds Converge*, BYTE, Feb. 1989, at 229. That price included 64K of Ram, two floppy disk drives and a monochrome monitor. *Id.* A computer of this type is capable of executing approximately 300 instructions per second. Daniel Ruby, *PCs and Crays Make an Odd Couple at a Weapons Lab*, PC WK., Apr. 30, 1985, at 47. Today, a computer based on Intel's Pentium processor can be purchased for less than $4,000. Jim Seymour, *Pentium: The Second Wave*, PC MAG., Jan. 25, 1994, at 110. The Gateway 2000 P5-60 can be purchased for $3,595. *Id.* at 135. That price includes 16 Megabytes of Ram, a 425 megabyte hard disk, two floppy disk drives, a CD-ROM drive and a high resolution color monitor. *Id.* A computer of this type is capable of executing about 100 million operations per second. John Burgess, *Cybertalk*, WASH. POST, May 24, 1993, at F19.

7. Computers are now found in 25 to 33 percent of the 96 million households in America. Nathan Cobb, *Where There's A Home PC, Odds Are There's A Software Pirate*, BOSTON GLOBE, Mar. 2, 1994, at 61.

8. *See infra* notes 14-17 and accompanying text.

malevolent software. Part III analyzes successful prosecutions under federal and state law, illustrating the difficulty of prosecuting an offender under current law. Part IV criticizes current legislation, highlighting its problems. Finally, Part V proposes a comprehensive overhaul of existing federal legislation and a move toward federalizing the law in this area.

I. MALEVOLENT SOFTWARE 101

A. What is Malevolent Software?

Researchers typically divide malevolent software into five categories: (1) "Trojan Horses," software that seems to be harmless but contains hidden malicious tendencies;[9] (2) "Worms," software designed to crawl through computer networks, repeatedly copying itself;[10] (3) "Logic Bombs," software similar to a Trojan Horse, that acts in response to certain stimuli;[11] (4) "Computer Viruses," software that attacks other files by modifying them so that they contain a copy of the virus;[12] and (5) "Stealth

---

9. Dawn Stover, *Viruses, Worms, Trojans, and Bombs: Computer "Infections,"* POPULAR SCI., Sept. 1989, at 59. An example would be if a user tried out a new computer game they had just received only to have their hard disk reformatted in the background during play. *Id.*

10. James W. Rawles, *The Viral Threat*, DEF. ELECTRONICS, Feb. 1990, *available in* LEXIS, Nexis Library, DEFELC File. Once the worm takes up residence, it may perform a variety of destructive activities against the host system including altering numerical database files or deleting or modifying other files. *Id.* Because worms are extremely slow and subtle, they are dangerously hard to detect. *Id.* An example of a worm is the software that Robert Tappan Morris planted on the Internet computer network. *See infra* notes 152-58 and accompanying text.

11. *See* Rawles, *supra* note 10. An example of a logic bomb is a piece of software that responds to the execution of an apparently harmless command entered on the computer by reformatting a computer's hard disk. *Id.* Some software vendors have begun to include disabling code in software written for commercial clients. Vicky H. Robbins, *Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software*, 10 COMPUTER LAW. 20, July 1993. This feature, a type of logic bomb, allows the software to be disabled at a later date by the vendor. *Id.* at 21. Vendors can use this capability to force a customer to satisfy contractual obligations, such as paying for the software. *Id.* at 22, n. 35 (citing Revlon v. Logisticon, Inc., No. 705933 (Cal. Super Ct.)).

12. *See* Rawles, *supra* note 10. A "boot virus" is a good example. This type of virus usually replaces the first track of a hard disk with a piece of itself, leaving the rest of the virus hidden elsewhere on the disk along with the real boot sector (the first track on the disk). *Id.* The virus is thus able to take control each time the computer is turned on, *i.e.*, booted. *Id.* It is then able to carry out its designed purpose as well as copy itself onto any floppy disks that may be inserted into the computer, thus allowing the virus to spread to other computers. *See* Stover, *supra* note 9, at 59. Viruses are generally considered to be the most dangerous type of malevolent software because they combine attributes of trojan horses, logic bombs and worms, all the while regenerating themselves. *See* Rawles, *supra* note 10. Unfortunately, the term "virus" is frequently applied incorrectly to every form of malevolent software, causing confusion regarding just what types of malevolent software are involved in any particular instance. *Id.*

Viruses," software similar to a Computer Virus but better able to hide itself and thus avoid detection.[13] Humans develop malevolent software—it is not a work of nature.[14] In fact, there are several groups, often collectively referred to as the "virus underground,"[15] who work to create, collect and distribute malevolent software throughout the United States and abroad.[16] Until recently, the fruits of these labors were even available on the U.S.

---

13. Michael Alexander, *Frodo Baggins: Rising From the Dead*, COMPUTERWORLD, July 23, 1990, at 4. An example is the 4096 virus, which has the ability to extract itself from an infected file if that file is being examined by an anti-virus program, thereby avoiding detection. *Id.* The "mutation engine" falls within this category as well. Rather than an actual virus, the mutation engine is an object module added to a virus that renders the virus undetectable. Peter Stephenson, *Preventative Medicine: Protecting Networks from Viruses*, LAN MAG., Nov., 1993, *available in* LEXIS, Nexis Library, LANMAG File. Instead of using the same algorithm to decript the code each time, a practice that allows virus detection software to identify a virus, the mutation engine uses a special algorithm to decript itself and the virus differently every time. *Id.* This makes standard anti-virus software useless. *Id.* At least three different mutation engines have already been discovered. *Id.*

14. Carol Ellison et al., *20 Utilities that Battle the Virus Threat*, PC MAG., Oct. 29, 1991, at 199. The first known computer virus was developed in 1983 by a student at the University of Southern California who was determined to prove that computer code could replicate itself, attach itself to other files and thereby change the behavior of the computer itself. *Id.* Some specialists believe that new viruses are currently being created at a rate of two or more a day! Josh Hyatt, *Computer Killers*, BOSTON GLOBE, Mar. 3, 1992, at 35. Because people ask why malevolent software creators persist, Michael Alexander, a senior editor at ComputerWorld arranged an interview with several of them to answer this question. *Id.* "[T]hey said they do it for the thrill of it. . . . They want to get their names out there they say, and if they cause damage that's just too bad." *Id.* One creator named "Garbage Heap" indicated that he believed virus writers should be afforded more respect. *Id.*

Malevolent software creators are not necessarily confined to any age or gender either. Harold Highland, an editor of *Computers & Security* magazine and Professor Emeritus of Computer Science at the State University of New York at Stony Brook stated that because of the sophistication of high school students and computer courses, "hackers are getting younger all the time." Laura DiDio, *A Menace to Society: Increasingly Sophisticated—and Destructive—Computer Viruses May Begin to Take Their Toll in Lives as Well as Dollars*, NETWORK WORLD, Feb. 6, 1989, at 71. One college professor, during a presentation to 16 year old high school students on viruses and what portions of a computer system should be protected from virus attacks, told of how one of the students interjected and said, "Well, if you're doing all that, I could still penetrate the video portion of the system." *Id.*

15. Wolfgang Stiller, *Wolfgang's World*, P.C. J., Mid-Jan. 1993, at 7.

16. *Id.* These groups have names such as Phalcon/Skism and Nuke. *Id.* Most groups based in the United States and Canada are composed of young boys, ages nine to sixteen, who lack the necessary skill to create new complex malevolent software but are readily capable of modifying existing malevolent software to escape detection by commercial viral scanning software. *Id.* Many of these groups even operate computer bulletin boards to allow their users to download malevolent software from their libraries. *Id.* While these groups modify existing malevolent software, most of the new and complex strains are being produced in countries that used to comprise the Eastern Bloc. *Id.*

In Bulgaria, a computer bulletin board system known as "The Virus Exchange" allows free access to its collection of over 300 viruses to anyone who uploads a new virus for the collection. Vesselin Bontchev, *The Bulgarian and Soviet Virus Factories*, (unpublished manuscript, on file with the *Washington University Law Quarterly*). *See also infra* note 22.

Department of the Treasury's Bureau of Public Debt Automated Information System computer bulletin board.[17]

Malevolent software is operating-system specific, meaning that a strain designed to run under DOS[18] cannot infect a computer running under another operating system.[19] Unfortunately, this has not limited the spread of malevolent software. Research reveals over 1,200 different strains targeted at IBM and IBM-compatible computers,[20] and many other strains designed to attack Amiga, Macintosh and Atari computers.[21] Although developers create malevolent software throughout the world, the United States, Bulgaria and the former Soviet Union are the top three countries of origin.[22] This widespread development network produces approximately

---

17. Laura Didio, *Debate Rages Over Posting Viruses on Electronic BBSes*, LAN TIMES, Aug. 9, 1993, *available in* LEXIS, Nexis Library, LANTME File. Kim Clancy, the system operator of the AIS BBS, is a security administrator who has ties to both the legitimate computer security community, as well as many underground hacker groups. *Id.* Using these contacts, she amassed a significant collection of virus source code and hacker "tools" that she made available to the general public. *Id.* Although Clancy claimed the public has a right to such information to help in the battle against malevolent software and hackers, her superiors felt otherwise, forcing her to remove all such files from the government operated BBS. *Id.* Ironically, Clancy had removed the replication portion of the virus source code, so the information was simply an incomplete blueprint in the hands of all but experienced hackers, who certainly do not need a public BBS to obtain such information. *Id.*

18. "DOS" stands for disk operating system. *See Glossary of Terms*, PC NOVICE, Premiere Issue, at 66. This is the software that allows applications to operate and interact with the computer's hardware. *Id.*

19. John Lateulere, *The Computer Virus Threat and What You Can Do About It*, CD-ROM PROF., Sept. 1992, at 105. In fact, malevolent software is so operating-system specific that it may only work under the version on which it was developed. *Id.* For example, a virus developed under DOS version 3.3 may not work under the more recent DOS version 6.2.

20. *Id.*

21. *Id.* Approximately 150 Amiga viruses, 30 Macintosh viruses, and several Atari ST viruses are also known to exist. *Id.*

22. *See* Ellison et al., *supra* note 14, at 201. A 1991 study designed to track the origin of frequently encountered viruses revealed that 41 virus strains had been developed in the United States, 38 strains in Bulgaria and 26 strains in the then Soviet Union. *Id.* Documented viruses have originated in 30 other countries as well. *Id.* Researchers believe that many Russian programmers create viruses because of the low demand for their services within the low-tech Russian economy. Gregory Gransden, *Boredom and Too Little Work May Be the Cause*, UPI, Oct. 26, 1992, *available in* LEXIS, Nexis Library, UPI File. Bulgarian researchers cite a decision made by their government to build computer hardware rather than software. *See* Bontchev, *supra* note 16. As a result, hardware was readily available during the 1980s, yet Bulgaria's Eastern Bloc status prevented most commercial software, developed in the West, from being lawfully sold within the country. *Id.* As a result, individuals would smuggle in one copy of a program, break the copyright protection scheme used on the diskettes and distribute the software throughout Bulgaria. *Id.* This practice created a large group of "quasi computer-programmers" who were bored with simply building computers. *Id.* As a result, they turned their talents toward creating malevolent software. *Id.*

100 new viruses or variations each month.[23]

B. *Transmission of Malevolent Software: The Basics of Infection*

Most computer software and hardware sold through retail channels is free of malevolent software.[24] Infection generally occurs after the user begins to operate the computer, and swaps diskettes with other computer users[25] thus exposing an infection-free computer to malevolent software present on a shared diskette. Other forms of data sharing—connecting to a network of other computers,[26] downloading files from a computer bulletin board

---

23. *See* Ellison et al., *supra* note 14, at 202.

24. There have, however, been several documented instances of hardware and software sold through retail channels containing malevolent software. For example, Leading Edge Products admitted that up to 6,000 computers shipped during the 1991 Christmas season may have been infected with a computer virus. Don Clark, *Thousands of Computers Infected with Virus*, S.F. CHRON., Jan. 25, 1992, at B1. Leading Edge officials claimed the virus was contracted from a software company that supplied it with software that was included on the computers' hard disks. *Id.*

One of the earliest documented infections of commercial software sold through retail channels involved Aldus Corporation. *News Shorts*, COMPUTERWORLD, Aug. 31, 1992, at 6. Thousands of copies of a software package sold by Aldus during 1988 were infected with a virus that flashed a peace message on users' screens. *Id.* Novell, during the final weeks of 1991, informed approximately 3,800 customers that it had released software that contained the Stoned III virus. Michael Alexander, *Shrink-Wrapped Viruses on Rise*, COMPUTERWORLD, Jan. 6, 1992, at 8. In fact, during 1991, over 100 occurrences of "shrink-wrapped" viruses were reported to McAfee Associates, a firm that produces anti-virus software. *Id.* Even computer industry powerhouse Intel has been affected. The company admitted in March 1992 that it had shipped 839 copies of a software package infected with the Michelangelo virus. *Michelangelo Virus Infects Intel Program*, S.F. CHRON., Mar. 3, 1992, at B2.

Commercially available CD-ROMs have also been struck by the virus bug. Susan Watts, *CD-ROM Users are Warned of Virus Threat*, THE INDEPENDENT, Jan. 3, 1994, at 4. The publishers of Software Vault Collection 2 and Night Owl 10, two CD-ROM collections of shareware, admitted their products contained viruses and they had plans to withdraw them from the market. *Id.*

25. An example of this is typical printer usage in an office. Anne Crawford, *Computer Virus Can Be Stopped*, CALGARY HERALD, Feb. 22, 1992, *available in* LEXIS, Nexis Library, CALHER File. Many offices have a single high-quality printer, which means that other workers bring their work to the computer connected to this printer. *Id.* If an infected disk is inserted into the computer connected to the printer, any malevolent software on the disk may take up residence in that computer. *Id.* When other users bring their work to the infected computer to obtain a printout, their diskettes are infected and the malevolent software is then transmitted to their computer as well when they return the disk to their own computer for later use. *Id.*

26. A LAN, local area network, is a type of computer network consisting of two to two hundred computers that are interconnected and communicate automatically without the use or need of floppy disks. *See id.* Since LANs are fully interconnected, if one node or stand-alone personal computer becomes infected, the malevolent software can spread rapidly throughout the entire network. Wayne Robertson, *The Best Defense Against Viruses May Be Sheer Luck*, NETWORK WORLD, Aug. 13, 1990, at 28. This means that the entire network of computers would need to be disinfected, resulting in excessive downtime and tremendous monetary costs depending on the size of the network. *Id.* The increasing number of LANs and WANs, wide area networks, means that the period of time it takes a

system,[27] or any other activity introducing new data into a computer from an external source[28]—may pose the risk of infection as well.

Although many strains of malevolent software originate overseas,[29] the globalization of the world economy has ensured that they will not remain confined to their geographic region of origin. International computer networks[30] and global travellers[31] further contribute to the ease with which malevolent software finds its way throughout the world in relatively

---

virus to spread can be accelerated up to one hundred times. *Computer Viruses: New Research Shows Epidemic Proportions*, EDGE: ON & ABOUT AT&T, Mar. 26, 1990, *available in* LEXIS, Nexis Library, EDGATT File. This problem can be further complicated when personal computers attached to a network also contain modems, allowing them to connect to outside sources, effectively creating a network within the network. Gene Reilly, *How Safe is Your Computer Network?*, MASS. LAW. WKLY., Oct. 19, 1992, *available in* LEXIS, Nexis Library, MALAWR File.

27. A computer bulletin board system (BBS) is made up of a computer system that can be accessed by other personal computers over telephone lines, using a modem. *Anti-Virus: Business Software Alliance, Citing Link to Computer Viruses, Plans Worldwide Campaign to Shut Down Illegal Bulletin Boards*, EDGE: WORK-GROUP COMPUTING REP., Nov. 27, 1992, *available in* LEXIS, Nexis Library, EDGWGC File. PC users that have connected to the BBS can download copies of software or electronic mail stored on the BBS to their own computers. *Id.* This widespread proliferation provides a fast and efficient method for creators of malevolent software to pass on their vicious products. *Id.* Typically, creators will hide their malevolent software inside of software that they place on the BBS. *Id.* When these infected programs are downloaded from the BBS to the users' computer, the malevolent software has succeeded in infecting yet another computer. *Id.* The rapid dissemination of malevolent software is thus quite possible through the use of BBSs which are often used by businesses to keep in contact with employees throughout the world. *See, e.g.*, Jeff Ubois, *Electronic Bulletin Boards Help Companies Communicate: BSSs Offer an Efficient, Cost-Effective Way to Exchange Information*, MACWEEK, Dec. 7, 1992, at 28. Software and hardware vendors also use them for product support throughout the world. *See, e.g. Software Support: WordStar Strengthens Technical Support Body*, EDGE: WORK-GROUP COMPUTING REP., Dec. 11, 1992, *available in* LEXIS, Nexis Library, EDGWGC File. Even the United States government has established numerous computer bulletin board systems. *See* Didio, *supra* note 17, at 1. The popularity of on-line services such as Compuserve, Prodigy and America Online, which together have over 3.5 million subscribers, illustrates the large number of people who utilize computer BBSs and similar on-line services. Glenn Rifkin, *At Age 9, On-Line Service Reboots*, N.Y. TIMES, Nov. 8, 1993, at C1.

28. Many malevolent software consultants caution against the use of pirated software or the use of diskettes brought from an employee's home to be used on an office computer. Lisa Kong, *I Am A Virus Buster*, STRAITS TIMES, Sept. 29, 1992, *available in* LEXIS, Nexis File, STRAITS File. One expert suggests that you should "[t]reat your diskettes like your toothbrush. Don't pass it around and don't share." *Id.*

29. *See supra* note 22 and accompanying text.

30. *See infra* note 40 and accompanying text.

31. *See* Ellison et al., *supra* note 14, at 201. Americans travelling overseas often purchase pirated copies of commercially-available software at prices far below market levels. *Id.* For example, current versions of Windows, Lotus 1-2-3 and other software packages can be purchased on the streets of Hong Kong, complete with photocopied documentation, for only a few dollars. Peter Stephenson, *Negotiating a Cure for Viruses: What the Law Cannot Do*, LAN TIMES, Sept. 6, 1993, *available in* LEXIS, Nexis Library, LANTME File.

short periods of time.[32]

Unintentional exposure to malevolent software is not the only threat today's computer user faces. Intentional attacks, implemented through the placement of malevolent software within a commercial software product[33] or on a computer network, must also be considered.[34] For example, a virus planted in the computer system used by the control tower of O'Hare Airport, triggered by a caller requesting to land a small private aircraft with a unique call sign, could activate a logic bomb,[35] crippling air traffic control computers.[36] While this scenario is fictitious only in the sense that it has not yet occurred, many researchers believe that malevolent software may be a useful terrorist weapon.[37] Even the United States armed forces have begun considering its possible uses.[38]

---

32. The 4096 virus was originally discovered in Israel. See Alexander, *supra* note 13, at 4. Approximately three months later it was discovered to have infected personal computers at Washington University in St. Louis. *Id.* This virus was also reported by Burger King franchises in California, Internal Revenue Service offices in Washington and a Houston-based bank. *Id.*

33. *See News Shorts*, *supra* note 24, at 6.

34. *See infra* notes 154-55 and accompanying text.

35. *See supra* note 11 and accompanying text.

36. *See* DiDio, *supra* note 14, at 71. While this scenario is only fictitious, the threat is certainly real. *Id.*

37. *Id.* While successful uses of malevolent software by terrorists have yet to be documented, some experts believe that such a threat exists. *Id.* The growth of computer technology has allowed the authors of malevolent software to become more technically sophisticated, and realistic terrorist targets include airports, hospitals and phone or power companies. *Id.* For example, malevolent software could be designed to disable AT&T's network of phone and trunk lines thereby disabling all telephone communication and data exchange that use phone lines. *Id.* In another scenario, a virus could be inserted into hospital computers resulting in the shutdown of life-support systems or the modification of patient records. *Id.* At an extreme level, a virus could be introduced into a military computer to prevent the proper use of a missile. *Id.* While malevolent software capable of such widespread damage would require the author to possess an extremely high level of technical proficiency, the possibility becomes more probable every day. *Id.* Other possible targets include computers used by banks, stock and commodity exchanges, as well as pension funds. *See* Rawles, *supra* note 10. *See also* W. John Moore, *Taming Cyberspace*, NAT'L. J., Mar. 28, 1992, at 745. A recent National Research Council study concluded that, "[t]omorrows terrorist may be able to do more damage with a keyboard than with a bomb." *Id.* This fear nearly became a reality in Japan where a plot to extort 25 million yen from a bank in Osaka using a computer virus was foiled. *Man Arrested for Attempting to Blackmail Credit Bank*, JAPAN ECON. NEWSWIRE, Oct. 4, 1993, *available in* LEXIS, Nexis Library, JEN File.

38. Application Configured Computers, an anti-virus software publisher and computer security consulting firm has been trying to interest the Department of Defense in a computer virus that imperceptibly alters the refresh rate of a monitor. *Forecast 1991*, COMPUTERWORLD, Dec. 24, 1990, at 72. This modification changes the refresh rate to a frequency that triggers headaches in users. *Id.* The company is suggesting that the virus be used against enemy radar operators. *Id.* Reports have also indicated that during the Gulf War, Iraqi air defense computers were disrupted through the use of computer viruses intentionally planted in memory chips of foreign made printers destined for Iraq. *See* Gransden, *supra* note 22, at 3.

C. *How Serious is the Problem?*

Malevolent software first gained widespread public notoriety in 1988, when a worm[39] paralyzed over 6,000 computers on the Internet[40] computer network.[41] The infection affected universities, military bases and research centers throughout the United States.[42] In addition to causing approximately $100 million of damages,[43] this incident illustrated the susceptibility of computer networks to infection.[44] Unfortunately, most computer users,[45] even those on the Internet, ignored the warning and allowed another malicious hacker[46] to gain unauthorized access to the network in 1990. This incident involved an attempt to damage a computer operated by the Harvard-Smithsonian Astronomical Observatory.[47] More recently, concerns have surfaced about Internet security in the wake of numerous cases of unauthorized access to computers operated by universities, the government and commercial entities, all of which are connected to the Internet.[48] As the number of Internet users continues to grow at an

---

39. *See supra* note 10 and accompanying text.

40. The Internet is a large network that connects over 5,000 networks throughout the United States and abroad and is used by five to ten million people. Carol Levin, *Traveling the Internet*, PC MAG., Jan. 26, 1992, at 71. Access to the Internet is relatively simple, requiring only a modem and a personal computer. John Markoff, *Traffic Jams Already on the Information Highway*, N.Y. TIMES, Nov. 3, 1993, at A1. The ease of access and interest in a "national data-highway" has dramatically increased usage of the Internet, which is now frequented by over 20 million users. Rick Tetzeli, *The Internet and Your Business*, FORTUNE, Mar. 7, 1994, at 86.

41. *See infra* notes 154-57 and accompanying text.

42. *See* Richard Raysman & Peter Brown, *Viruses and How to Prevent Them*, N.Y. L.J., Sept. 12, 1989, at 3.

43. Nicholas Spill, *Immunized Testimony: How to Beat Those Lousy Viruses*, LEGAL TIMES, Sept. 17, 1990, at S31. Interestingly, Robert Tappan Morris, the individual convicted under the CFAA for releasing the worm, is the son of Robert Morris, Sr., the chief scientist in charge of computer security at the National Computer Security Center, a branch of the National Security Agency. *Id.*

44. After the Internet infection, the World Bank discovered that its computer network operating system was susceptible to the same type of worm. *See* DiDio, *supra* note 14, at 72.

45. Many well-known banks and computer manufacturers continued to use the same operating system employed on the Internet, without correcting the flaws Morris exploited. *Id.*

46. The term "hacker" is often used to describe individuals who employ their computer expertise illegally to manipulate computers and software. *See, e.g.*, William G. Flanagan & Brigid McMenamin, *The Playground Bullies are Learning How to Type*, FORBES, Dec. 21, 1992, at 184.

47. Bob Brown, *Internet Hacker Frustrates Users, Eludes Detection*, NETWORK WORLD, Mar. 26, 1990, at 4. The hacker indicated that he was trying to attack Clifford Stoll, the computer system manager at the Observatory, who had recently written a book about hackers characterizing them in a manner deemed unacceptable by this individual. *Id.*

48. John Markoff, *A Dose of Computer Insecurity*, N.Y. TIMES, Nov. 1, 1993, at C1. Although these intrusions have not had serious repercussions, one New York City on-line service was forced to

exponential pace,[49] so do the number of attempts at gaining unauthorized access to the Internet[50] and other networked systems.[51]

Some downplay the threat posed by malevolent software,[52] while others suggest that anti-virus software manufacturers exaggerate the problem to increase sales.[53] Although the low number of successful prosecutions of malevolent software creators may support these positions,[54] most infections go unreported.[55] Moreover, even if infections are reported, it remains difficult to identify the responsible party.[56] A recent National Computer Security Association survey found that sixty-three percent of user sites polled had experienced problems associated with computer viruses.[57]

---

shut down for three days to correct problems related to the incidents. *Id.*

49. Estimates place the number of Internet users around 20 million, *see* Tetzeli, *supra* note 40, at 86, a figure that grows by as much as 15% a month. Michael W. Miller, *Contact High*, WALL ST. J., Nov. 15, 1993, at R4.

50. Jared Sandberg, *Computer 'Cracking' Is Seen on the Rise*, WALL ST. J., Nov. 1, 1993, at B5. The Computer Emergency Response Team, an organization formed after the Morris incident, logged 773 security breaches during 1992, and currently deals with three to four breaches everyday. *Id.*

51. Jerry Seper, *4 Arrested in Denmark for Computer Hacker Scheme*, WASH. TIMES, Dec. 16, 1993, at A5. An on-line survey undertaken by the ComSec BBS, a nonprofit organization with over 2,100 members who are computer security professionals around the world, reveals just how serious the problem has become. Laura Didio, *Security Deteriorates as LAN Usage Grows*, LAN TIMES, April 5, 1993, *available in* LEXIS, Nexis Library, LANTME File. Of those who responded, 69% experienced a computer security problem during the past year, 53% of the problems resulted in a loss of $10,000 or more. *Id.* Fifty-nine percent of the respondents had been hit by a computer virus in the past year, with 9% of the attacks costing more than $100,000. *Id.* The ComSec BBS can be reached at (415) 495-4642, modem settings 8,N,1. *Id.*

52. Some technology experts believe that the notoriety computer viruses have received is simply the result of the media attempting to find a hot story. Ellen Chaffin, *An Epidemic Real or Imagined*, INC. MAG., Apr. 1989, at 36.

53. *See* Hyatt, *supra* note 14, at 35. Central Point Software Inc., one of many anti-virus software manufacturers, developed a special Michelangelo protection kit, available for $29, that was marketed to combat the Michelangelo virus threat. *Id.* *See infra* notes 71-78 and accompanying text. The corporation also set aside $250,000 for a national advertising campaign in an effort to depict a high level of customer service to draw customers back. *Id.* One national software chain reported that sales of anti-virus software increased 3000% during the week prior to Michelangelo's scheduled trigger date. Lateulere, *supra* note 19, at 105.

54. *See infra* part III.

55. *See* Flanagan & McMenamin, *supra* note 46, at 186. Most victims, particularly businesses, remain quiet for fear of looking foolish or inviting a copycat to strike again. *Id.* *Law and Order* magazine estimates that only 11% of all computer crime is reported. *Id.*

56. *Id.*

57. Gary H. Anthes, *Viruses Continue to Wreak Havoc at Many US Companies*, COMPUTERWORLD, Jun. 28, 1993, at 52. The average attack affected 142 PCs, and required over two days to remedy. The figures were released as part of the kickoff on Capital Hill for Virus Awareness Day (June 9). *Id.* Over 600 end-user locations that operate more than 300 PCs per site were polled by the National Computer Security Association for this study. Mick Donahoo and Blaine Homer, *Quarantined*

NASA,[58] the Defense Data Network,[59] the Second Circuit Court of Appeals,[60] a Fortune 500 insurance company,[61] Capitol Hill,[62] IBM,[63] the White House,[64] a British nuclear power plant,[65] a traffic signal in Louisiana,[66] and small businesses throughout the United States have reported infections.[67] The U.S. Department of Commerce has recorded approximately seventy-six attacks on its computers from nineteen different

---

Area: Tackling Viruses NLM-Style, LAN TIMES, Aug. 9, 1993, *available in* LEXIS, Nexis Library, LANTME File.

58. COMM. DAILY, Apr. 8, 1992, *available in* LEXIS, Nexis Library, COMDLY File. A security lapse during 1989 allowed a virus to infect NASA as well as other scientific agencies. *Id.*

59. *Big Guns Take Aim at Virus*, GOV. COMPUTER NEWS, Nov. 21, 1988, *available in* LEXIS, Nexis Library, GOVCMP File. Computers in Arlington, Virginia, the Lawrence Livermore Labs in California, the Naval Ocean Systems Command in San Diego and the Naval Research Lab in Maryland were hit by this virus as well. *Id.*

60. Deborah Pines, *Federal, State Courts Attack Computer Virus and Prevail—So Far*, N.Y. L.J., Mar. 4, 1992, at 1. A virus called "Stoned" has been discovered on all six computers housed in the Second Circuit library as well as fifteen of the seventeen computers employed by Second Circuit staff attorneys. *Id.* Numerous other strains of malevolent software have also appeared in courthouse staff offices as well as judges' chambers. *Id.*

61. Franklynn Peterson and Judi K. Turkel, *Who Says the Michelangelo Virus Was a Bust?*, STAR TRIB., Mar. 12, 1992, at 2D. The company found that 20% of its personal computers were infected with the virus. *Id.* Had the virus erased the data on the infected personal computers, the company could have been in jeopardy of going out of business. *Id.*

62. Malevolent software infected a bank of computers used by Senators and Representatives. Emily Brower, *House Considers Tougher Laws to Combat Computer Viruses*, MACWEEK, Mar. 14, 1989, at 6.

63. In 1986, thousands of computers connected to IBM's worldwide network were tied up by malevolent software that sent out Christmas greetings. *See* Gransden, *supra* note 22, at 3.

64. *Health-Care Plan on Computer Disks Spreading 'Virus'?*, PUBLISHER MAG., Nov. 6, 1993, at 13. Bloomberg Business News reported that disks it received from the White House containing President Clinton's health-care reform plan apparently came with an unwanted copy of the Stoned III virus. *Id.*

65. Nick Nuttall, *Virus Slips Nuclear Plant PC Security*, S. CHINA MORNING POST, Nov. 23, 1993, *available in* LEXIS, Nexis Library, SCHINA File. Sizewell B, Britain's most advanced nuclear power station was infected by a virus that plays "Yankee Doodle Dandy." *Id.*

66. Richard Boyd, *Signal Trouble Causes Gridlock on Gause*, TIMES-PICAYUNE, April 6, 1993, at B1. A virus was discovered in the control panel of a set of intersection traffic lights. *Id.* In several instances, the virus switched the traffic signals from timed sequences to flashing, causing traffic jams. *Id.*

67. A small accounting firm in New Jersey discovered the Michelangelo virus during the height of tax season. *Id.* In fact, estimates indicate that for each firm that detected Michelangelo, two others detected that another virus had infected their computers. *Id.* Several banks and thrifts in Pennsylvania, New Jersey, Maryland, and Kentucky were the apparent target of a hacker calling himself Master Fard Muhammed. *Tech Roundup: Beware of Holiday Virus*, NAT'L MORTGAGE NEWS, Dec. 20, 1993, *available in* LEXIS, Nexis Library, NMN File. Master Fard mailed disks containing a virus to these financial institutions, which unknowingly loaded apparently legitimate software onto their computers, only to find they had been infected with a powerful stealth virus. *Id.*

viruses since 1988.[68] The Gorky Automobile Works in the former Soviet Union reported an infection during 1988,[69] and Japan has recently reported tremendous increases in damage caused by malevolent software.[70]

Malevolent software was the focus of the international news media during the Michelangelo[71] scare of 1992.[72] Although Michelangelo is not a new virus, and remains a threat on March 6th every year,[73] the news media seized upon it during 1992, perhaps because of the gaining popularity of personal computers.[74] While this coverage helped avert most of the possible damage,[75] computer users in South Africa,[76] Argentina[77] and Germany[78] reported infections and data loss.

Although losses associated with infections are typically described in terms of downtime and lost data,[79] policy-makers must also consider resources expended on preventive measures.[80] Software scanning devices[81] and hardware-based solutions are readily available.[82] Most of

---

68. *See* Lateulere, *supra* note 19, at 107. During October 1991, employees at the Commerce Department spent 200 work hours recovering data lost to viruses. *Id.* The work during that month alone exceeded the total time spent during 1990 recovering data lost in a similar manner. *Id.*

69. Sanford Sherizen, *Bozhe Moy Hackers and Viruses Already Plague Soviets*, COMPUTERWORLD, Aug. 20, 1990, at 74. In that case, an unidentified programmer allegedly used a virus to shut down an assembly line as retaliation for a dispute over working conditions in the plant. *Id.* He was tried and convicted under Article 206, the Hooliganism Law, carrying a sentence of up to six years in jail. *Id.*

70. *Computer Contamination by Viruses More Than Triples*, JAPAN ECON. NEWSWIRE, Dec. 22, 1993, *available in* LEXIS, Nexis Library, JEN File. An agency of the Ministry of International Trade and Industry expects to log around 900 infections during 1993, up from 253 cases in 1992. *Id.*

71. The virus is named for the Renaissance master himself and is triggered on his birthday, March 6th. *Michelangelo Attacks Some PCs Early*, S.F. CHRON., Mar. 6, 1992, at B2.

72. During the weeks preceding March 6, 1992, media coverage of the Michelangelo virus was extensive. Jonathan Weber, *Most Escape Brush with 'Michelangelo,'* L.A. TIMES, Mar. 7, 1992, at A1.

73. *Id.*

74. *See generally* Cobb, *supra* note 7.

75. *See* Weber, *supra* note 72, at A1. Most of the victims of the virus were small businesses and home personal computer users that had missed or ignored the numerous warnings in the press. *Id.*

76. Approximately 1,500 computers that made up a network of pharmacies in South Africa were hit by the virus. *Id.*

77. One newspaper in an Andean resort area reported the virus had destroyed files on its computers. *See Michelangelo Attacks Some PCs Early*, *supra* note 71, at B2.

78. The German government reported that approximately 80 computers were hit there. *See* Weber, *supra* note 72, at A1.

79. *See generally* Anthes, *supra* note 57.

80. Expenses of this type refer to the purchase of software and hardware protection devices, time spent backing up data and time spent educating computer users about the threat of malevolent software.

81. Patrick Honan, *Avoiding Virus Hysteria*, PERS. COMPUTING, May 1989, at 84. There are numerous virus detection programs on the market that provide an affordable way to monitor and eliminate potential infections. *Id.* However, these packages are typically only effective against the most common types of viruses. *Id.*

these products, however, defend only against known strains of malevolent software and may be unable to detect and defend against new variations.[83] To insure the best protection available, computer users must purchase product updates at least two to three times a year.[84] Lloyds of London even offers an insurance policy to cover losses for users resigned to the belief that their data will be destroyed by malevolent software.[85]

Estimates suggest that yearly losses associated with malevolent software will reach $2 billion during 1993 and continue to increase.[86] Furthermore, damage calculations may soon include the loss of human life as our society increases its reliance on computers.[87] The ease of access to the Internet and the availability of phone numbers allowing remote computer users to access computer networks operated by branches of the United States government and armed forces further exacerbates the problem.[88] Although many of these networks are not vital to our government or national

---

Software scanning devices are generally divided into three categories: (1) filter programs, designed to remain in a computer's memory and monitor operations to prevent unauthorized modifications to files; (2) infection detection programs, designed to take a picture of the user's system from time to time and make comparisons, notifying the user of any changes; and (3) virus removal programs, designed to recognize and destroy common viruses. *See* Stover, *supra* note 9, at 62. One malevolent software creator took advantage of the ready availability of virus detection software on computer bulletin boards and created a strain of malevolent software that was designed to appear and function like an anti-virus scaner, while it destroyed data on the user's hard disk. *Id.* at 61.

82. Zeus Corporation makes a plug-in circuit board that is designed to check for viruses on IBM compatible computers. *See* Stover, *supra* note 9, at 62. American Computer Security Industries produces what it calls the "Immune System," a computer the company claims is virus proof due to hardware components that prevent modification to the operating system. *Id.*; *see generally* Ellison, *supra* note 14 (illustrating the large number of software scanning devices available).

83. *See* Rawles, *supra* note 10, at 63.

84. *Id.*

85. *See* Stover, *supra* note 9, at 60.

86. James Daly, *Virus Vagaries Foil Feds*, COMPUTERWORLD, July 12, 1993, at 1.

87. Scott Mace, *I Swear . . .: Consumers, Legislators and Publishers are Considering Establishing Rules to Cover Programmers*, INFOWORLD, Jan. 1, 1990, at 30. Mace cites the public's reliance on computer aided drafting (CAD) and medical software. *Id.*; *see also* text accompanying notes 35-36.

88. By logging onto the PC Innovators bulletin board, which can be reached at (314) 939-6404, modem settings 8,N,1, the author was able to download a list of military computer systems accessible using a modem and standard phone line. For example, using the appropriate area code, Edwards Air Force Base can be reached at 527-3249, modem settings 8,N,1. The United States Air Force Training Command may be reached at the appropriate area code by dialing 478-6727, modem settings 8,N,1. This list also contains several toll-free numbers that can be easily reached from anywhere in the world. [list on file with the *Washington University Law Quarterly*]. Hackers who do not have such a list employ telephone directory search programs to locate networks or bulletin board systems, many of which are restricted systems. *See* Reilly, *supra* note 26. These programs simply dial number after number until a modem answers, thus allowing them to locate even unlisted computer dial-in lines. *Id.*

security, their proximity to such networks should cause concern.[89]

It is no longer appropriate to ask *if* there is a problem: cost estimates that reach $2 billion,[90] federal legislation,[91] state legislation in forty eight states,[92] a National Virus Awareness Day,[93] and over 90,000 reported infections in a calendar year[94] clearly illustrate that a problem exists. The correct inquiry is how to address this problem.

II. THE LEGAL ENVIRONMENT

A. Federal Legislation

The Computer Fraud and Abuse Act of 1984 (CFAA),[95] marked the first attempt to regulate computer fraud and the creation of malevolent software at the federal level. The CFAA prohibits unauthorized access to computers that contain classified material or information that could be used to obtain monetary gain.[96] In response to the proliferation of personal computers during the two years after its enactment, the CFAA was

---

89. While these systems and others on the list obtained by the author may not contain or operate systems vital to the nation's protection, if one were infected with malevolent software and a disk that was used in the infected computer was placed into another computer on another network, that network could be infected as well. The multiplicity of transmission is endless because the military makes extensive use of networks. *See* Reilly, *supra* note 26. *2600*, a Long Island, New York-based quarterly journal for computer users has listed private phone numbers for the White House and Pentagon since 1984. *See* DiDio, *supra* note 14, at 72. Articles have also appeared that provide diagrams for building electronic listening devices and equipment to bypass phone circuitry to make free calls. *Id.* Recently, articles on writing and defending against viruses have been published. *Id.*

90. *See* Daly, *supra* note 86, at 1.

91. *See infra* part II.A.

92. *See infra* part II.B. Interestingly enough, neither Washington D.C. nor Vermont currently has computer crime legislation. While it seems safe to assume that most computers in Washington D.C. would fall within the protection of the CFAA, such is not the case in Vermont.

93. *Viruses*, INFO. WEEK, June 14, 1993 at 10. On June 9, 1993, Vice President Al Gore, champion of the data superhighway, spoke as part of a full day of events focusing on the increasing prevalence of computer viruses. *Id.* The event was co-sponsored by 3M and the National Computer Security Association. *Id.*

94. *See* Stover, *supra* note 9, at 60. Hardware and software manufacturers have also formed a consortium, The Computer Virus Industry Association, to combat malevolent software. *Get Information and Help to Fight Viruses*, LAN TIMES, Nov. 19, 1990, *available in* LEXIS, Nexis Library, LANTME File.

95. 18 U.S.C. § 1030 (Supp. I 1992). Prior to passage of the CFAA, mail and wire fraud statutes were used to prosecute those charged with computer abuse. S. REP. NO. 544, 101st Cong., 2d Sess. 2 (1990).

96. S. REP. NO. 544, *supra* note 95, at 2.

amended in 1986.[97] The amendments clarified portions of the earlier law and expanded protection to include prohibitions on the destruction or alteration of data by unauthorized users.[98] Technological evolution again out-paced the CFAA during the late 1980s and early 1990s however,[99] resulting in the initiation of several unsuccessful legislative remedies.[100] To date, the CFAA remains operative as amended in 1986.[101]

The CFAA applies solely to "federal interest computers," defined as: (1) computers used exclusively by the federal government; (2) computers used exclusively by financial institutions; and (3) computers involved in interstate computer crimes.[102] Violation of the CFAA occurs when

---

97. S. REP. NO. 432, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. at 5945. For a more in-depth review of The Computer Fraud and Abuse Act of 1986, see Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453 (1990).

98. S. REP. NO. 544, *supra* note 95, at 2.

99. *Id.* On May 15, 1989, William S. Sessions, then-FBI Director, and Dr. Clifford Stoll of the Harvard-Smithsonian Center for Astrophysics, testified before the Senate Subcommittee on Technology and the Law. *Id.* Notable was Dr. Stoll's testimony regarding his apprehension of a West German spy using computer networks within the United States to attempt to gain access to military information. *Id.* at 3. Dr. Stoll also described how his research at the Center "was halted when Robert Morris, Jr. introduced a computer 'worm' on to the Internet computer network in November 1988." *Id.* at 5.

The General Accounting Office also reported in 1989 that it was unclear whether all virus related incidents would fit within the scope of the CFAA. Michael Alexander, *Computer Law Unclear, GAO Finds*, COMPUTERWORLD, July 31, 1989, at 8. The core of the CFAA also suffers from a lack of clarity with regard to offenses differentiated on the basis of "authorized" or "unauthorized" access, terms that are not defined within the CFAA. Scott Charnet, *What's Wrong With the Computer Crime Statute?*, COMPUTERWORLD, Feb. 17, 1992, at 33.

100. A set of proposed amendments were offered on the Senate floor in 1990. S. 2476, 101st Cong., 2d Sess. (1990). The Senate Committee on the Judiciary passed them in 1991 but they were not considered by the House of Representatives during the 101st Congress. 138 CONG. REC. S17,806 (daily ed. Oct. 8, 1992) (statement of Sen. Leahy). The amendments were subsequently reintroduced to the 102d Congress, *see* S. 1322, 102d Cong., 2d Sess. (1992), passed by the Senate as an amendment to the Violent Crime Control Act, *see* S. 1241, 102d Cong., 2d Sess. (1992), and by the House Committee on the Judiciary as part of the conference report to H.R. 3371, *see* 139 CONG. REC. S16,421 (daily ed. Nov. 19, 1993) (statement of Sen. Leahy). See *infra* notes 230-35 and accompanying text for a complete discussion of the amendments.

During this same time period, the Computer Virus Eradication Act of 1989, H.R. 55, 101st Cong., 1st Sess. (1989), and the Computer Protection Act 1989, H.R. 287, 101st Cong., 1st Sess. (1989), were introduced to Congress. Both bills ultimately died.

101. Although several minor amendments have been made since the substantive changes in 1986, the form and focus of the CFAA have remained unchanged.

102. 18 U.S.C. § 1030(e)(2) (Supp. I 1992). Congress declined to enact sweeping federal legislation stating that it believed the federal interest standard struck an "appropriate balance" between federalism and state sovereignty. *See* S. REP. NO. 432, *supra* note 97, at 4, *reprinted in* 1986 U.S.C.C.A.N. at 2482.

anyone: (1) obtains restricted information,[103] by knowingly or intentionally accessing a computer without authorization or exceeding their authorization with intent or reason to believe the information will be used against the United States or to the benefit of a foreign nation;[104] (2) obtains information from a financial institution or other delineated organization by intentionally accessing a computer without authorization or exceeding their authorization;[105] (3) intentionally and without authorization, accesses a computer of a department or agency of the United States government and affects its use;[106] (4) obtains anything of value and furthers any intended fraud by knowingly accessing a federal interest computer without authorization or by exceeding authorized access;[107] (5) alters, damages or destroys information or prevents any authorized use of such information, by intentionally accessing a Federal interest computer without authorization;[108] or (6) knowingly and with fraudulent intent traffics in any information, including passwords, through which computers may be accessed without authorization, if it affects interstate commerce or a computer used by or for the United States government.[109] Sentencing guidelines[110] divide the six offenses into three categories, applying punishment based on the categorical violation.[111] Repeat offenders receive enhanced penalties only if their second violation falls within the

---

103. "Restricted data" includes any information that has been designated as deserving of such protection by executive order or statute, whether it be for reasons of national defense, foreign relations or any other purpose. 18 U.S.C. § 1030(a)(1) (Supp. I 1992).

104. *Id.*

105. *Id.* § 1030(a)(2).

106. *Id.* § 1030(a)(3). Intentionally accessing a computer without authorization that is not exclusively used or owned by the United States government is also included if such access affects the government's use of the computer. *Id.*

107. *Id.* § 1030(a)(4). This provision is not satisfied if the sole object of the fraud or the thing of value obtained consisted only of use of the accessed computer. *Id.*

108. *Id.* § 1030(a)(5). In addition, the unauthorized access must cause a loss aggregating $1,000 or more during a single year or impair, modify, or potentially impair or modify the medical care or treatment of at least one individual. *Id.* For example, in 1983, a group known as the "414 Gang" broke into the Memorial Sloan-Kettering Cancer Center computer system in New York, thereby gaining access to radiation treatment data on over 6,000 patients. S. REP. NO. 432, *supra* note 97, at 2-3, *reprinted in* 1986 U.S.C.C.A.N. at 2480. The Senate Committee on the Judiciary intended the CFAA to apply to this situation because the "414 Gang" had access to radiation treatment levels for all patients, and could have altered them. *Id.*

109. 18 U.S.C. § 1030(a)(6) (Supp. I 1992).

110. *Id.* § 1030(c).

111. Category one contains violations of section (a)(1), category two contains violations of sections (a)(2), (a)(3) and (a)(6), and category three contains violations of sections (a)(4) and (a)(5). *Id.*

same category as their first.[112]

The nature of the specific acts proscribed by the CFAA and the statute's failure to address the creation and transmission of malevolent software limits its applicability to malevolent software creators. In fact, by its nature, the act of creating or transmitting malevolent software could constitute a violation of the CFAA *only* if: (1) it accesses and negatively affects the government's operation of a computer;[113] or (2) accesses and destroys or alters information contained in a "federal interest" computer.[114]

In addition to the problem of limited applicability, all causes of action brought under the CFAA require proof of *intentional unauthorized access to a computer.*[115] If one traces the typical evolution of a strain of malevolent software from creation to infection,[116] it becomes obvious that most malevolent software creators intend to access only (as defined by the CFAA) a single computer. Subsequent infections of additional computers are usually a byproduct of the creator's actions, initiated by an individual, other than the creator, who unknowingly places an infected diskette into a computer the individual is authorized to use.[117]

Malevolent software begins as "code"[118] on the creator's computer. After perfecting the software, the creator then releases it, usually by embedding it in a file meant for public distribution.[119] Infection occurs when another computer comes in contact with the infected file.[120]

---

112. *Id.* § 1030(c)(1)(B)-(c)(3)(B).

113. *See supra* note 106 and accompanying text. Penalties for such a violation include a fine or imprisonment for not more than one year. 18 U.S.C. § 1030(c)(2)(A) (Supp. I 1992). Repeat offenders face a fine or imprisonment for not more than ten years, or both. *Id.* § 1030(c)(2)(B).

114. *See supra* note 108 and accompanying text. Penalties for such a violation include a fine or imprisonment for not more than five years, or both. 18 U.S.C. § 1030(c)(3)(A) (Supp. I 1992). Repeat offenders under this subsection face a fine or imprisonment for not more than ten years, or both. *Id.* § 1030(c)(3)(B).

115. *See* 18 U.S.C. § 1030(a) (Supp. I 1992).

116. For purposes of this Note, the term "infection" is used to describe the process by which malevolent software becomes embedded in a file or elsewhere within a computer.

117. Infection may occur under other circumstances as well. This example is presented only to illustrate one possibility. Robert Tappan Morris, Jr. used a similar argument defending his actions that led to the infection of the Internet Network. *See infra* notes 164-66 and accompanying text.

118. For purposes of this Note, the term "code" will be used to refer to various programming languages used by computer programmers.

119. Files intended for public distribution may include portions of a commercial software package or even files posted freely on a computer bulletin board. *See supra* notes 16, 24.

120. John Markoff, *Worms and a Garden of Eden*, HOUSTON CHRON., Mar. 9, 1992, *available in* LEXIS, Nexis Library, HCHRN File.

Infection typically involves the replication of the malevolent software onto the computer's hard disk or elsewhere in the computer itself.[121] Once resident, the malevolent software may destroy or alter data or perform any of a number of destructive tasks.[122] Additionally, once malevolent software infects a computer, it usually replicates itself onto any floppy disk that may be used in the computer.[123] This feature makes it possible to spread the infection from one computer to others.[124] The creation and transmission of malevolent software thus cannot be readily described as intentional unauthorized computer access in the case of each infection because the malevolent software creator does not personally access each computer that is infected.[125] Arguably, a creator has only accessed the computer to which they first introduced the infected file. This same line of argument can also be applied to the intent requirement of the CFAA.

Poorly drafted provisions threaten to diminish other areas of protection as well. The CFAA defines "computer" to exclude automated typesetters and typewriters as well as hand held calculators and other similar portable devices.[126] This ambiguous distinction arguably excludes laptop and palmtop computers because of their portability.[127] While the CFAA prohibits the alteration or destruction of "information," it fails to indicate whether data in RAM, the computer's memory,[128] is protected or whether only data stored on a disk or other storage medium falls within the CFAA's ambit.

---

121. *Id.*

122. *Id.* For example, Cascade.1701 causes text on a color screen to fall to the bottom line. *The Top Viruses*, NETWORK WORLD, July 27, 1992, at 40. Cascade.1704 causes a computer to randomly reboot. *Id.* Green Caterpillar.1 causes a green caterpillar to appear in response to a "DIR" or "COPY" command. *Id.* Jerusalem.Standard deletes files on Friday the 13th; several new versions perform similar operations on various dates. *Id.* Michelangelo, a derivative of Stoned.Standard, deletes all files on the boot drive on March 6th. *Id.* Yankee Doodle 2885 plays "Yankee Doodle" at 5:00 p.m. through the computer's speaker every day, but causes no damage. *Id.*

123. *See* Markoff, *supra* note 120.

124. *Id.*

125. *See, e.g.*, United States v. Morris, 928 F.2d 504, 509-10 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991).

126. 18 U.S.C. § 1030(e)(1) (Supp. I 1992).

127. The author is referring to products such as the Z-Lite 320L. The Z-Lite 320L is a four pound subnotebook computer containing two megabytes of RAM and a 60 megabyte hard disk. Greg Pastrick, *Z-Lite 320L: 4 Pounds of Good Looks, Smart Features*, PC MAG., Feb. 23, 1993, at 59. The Z-Lite is based on the Intel 386 microchip. *Id.*

128. RAM refers to the computer's dynamic memory. *Glossary of Terms*, *supra* note 17, at 67. Information is stored here only temporarily and is lost when power is turned off. *Id.*

B. State Legislation

Congressional rejection of an all encompassing computer crime law[129] forced states to enact legislation protecting computers falling outside of the "federal interest" computer classification.[130] Some states revised the definition of "property" to include information stored on a computer or floppy disk[131] while one state has classified computer crime as an offense against intellectual property.[132] Most states, however, have enacted statutes similar in scope to the CFAA.[133] In a few instances, states[134] have expanded coverage by developing statutes that specifically proscribe the creation and transmission of malevolent software.

States that have attempted to combat malevolent software by broadening the definition of the term "property" typically follow the approach taken by Massachusetts.[135] Massachusetts defines property to include electronically-processed or stored data.[136] Offenders are prosecuted under existing legislation proscribing theft, embezzlement or conversion.[137] Alabama and Wyoming classify electronically-processed or created data as intellectual property[138] and prosecute computer crimes as violations of intellectual property rights.[139] While these approaches may prove successful against malevolent software that destroys, alters or acts upon presently existing data contained within a computer,[140] these statutes may be ineffective against malevolent software that displays annoying messages or plays songs.[141]

Most states have adopted legislation modeled closely after the

---

129. *See* S. REP. NO. 432, *supra* note 97, at 4, *reprinted in* 1986 U.S.C.C.A.N. at 2482.

130. *See supra* note 102 and accompanying text.

131. Raysman & Brown, *supra* note 42, at 6. *See infra* notes 135-37 and accompanying text.

132. Raysman & Brown, *supra* note 42, at 6. *See infra* notes 138-39 and accompanying text.

133. Raysman & Brown, *supra* note 42, at 6. *See supra* notes 102-112 and accompanying text.

134. *See infra* notes 144-46 and accompanying text.

135. States that have adopted this approach include: Arkansas, *see* ARK. CODE ANN. §§ 5-41-101 to -107 (Michie Supp. 1991); Georgia, *see* GA. CODE ANN. §§ 16-9-90 to -94 (1992); Massachusetts, *see* MASS. GEN. LAWS ANN. ch. 266, § 30 (West 1988); and Washington, *see* WASH. REV. CODE ANN. § 9A.52.110-.130 (West 1988).

136. MASS. GEN. LAWS ANN. ch. 266, § 30 (West 1988).

137. *See generally* MASS. GEN. LAWS ANN. ch. 266, § 30(1) (West 1988).

138. *See* ALA. CODE §§ 13A-8-100 to -103 (Supp. 1992); WYO. STAT. §§ 6-3-501 to -505 (1988).

139. *See, e.g.*, ALA. CODE § 13A-8-102.

140. *See supra* notes 9-13 and accompanying text for differentiation between specific actions taken by malevolent software.

141. *See* Raysman & Brown, *supra* note 42, at 6.

CFAA.[142] In most cases, these statutes go no further toward defining malevolent software or proscribing it than the CFAA and thus suffer from the same shortcomings.[143] Some states in this group, however, include specific definitions and provisions addressing malevolent software within their computer crime legislation.[144] For example, Minnesota prohibits the distribution of "destructive computer programs,"[145] defined as any program that degrades computer performance, destroys data, produces unauthorized data, performs unauthorized alterations on data or produces another destructive computer program.[146] These statutes are more effective than those modeled after the CFAA. Nevertheless, prosecutors

142. States that have taken this approach include: Alaska, *see* ALASKA STAT. § 11.46.740 (1989); Arizona, *see* ARIZ. REV. STAT. ANN. § 13-2316 (1989); Colorado, *see* COLO. REV. STAT. ANN. §§ 18-5.5-101 to -102 (West 1990 & Supp. 1992); Connecticut, *see* CONN. GEN. STAT. ANN. §§ 52-570b, 53a-250 to -261 (West 1985); Delaware, *see* DEL. CODE ANN. tit. 11, §§ 931-939 (1987 & Supp. 1992); Florida, *see* FLA. STAT. ANN. §§ 815.01-.07 (West Supp. 1993); Hawaii, *see* HAW. REV. STAT. §§ 708-890 to -893 (Supp. 1992); Idaho, *see* IDAHO CODE §§ 18-2201 to -2202 (1987); Indiana, *see* IND. CODE § 35-43-1-4 (Supp. 1992); Iowa, *see* IOWA CODE ANN. §§ 716A.1-.16 (West Supp. 1993); Kansas, *see* KAN. STAT. ANN. § 21-3755 (1988); Kentucky, *see* KY. REV. STAT. ANN. § 434.840-.860 (Baldwin 1985); Louisiana, *see* LA. REV. STAT. ANN. §§ 14:73.1-.5 (West 1986 & Supp. 1993); Maryland, *see* MD. CODE ANN., CRIM. LAW § 146 (1988 & Supp. 1993); Michigan, *see* MICH. COMP. LAWS ANN. §§ 752.791-.797 (West 1991); Mississippi, *see* MISS. CODE ANN. §§ 97-45-1 to -7 (Supp. 1991); Missouri, *see* MO. ANN. STAT. §§ 569.093-.099 (Vernon Supp. 1993); Montana, *see* MONT. CODE ANN. §§ 45-6-310 to -311 (1991); Nebraska, *see* NEB. REV. STAT. §§ 28-1343 to -1348 (1992); Nevada, *see* NEV. REV. STAT. ANN. § 207.477 (Michie 1991); New Hampshire, *see* N.H. REV. STAT. ANN. §§ 638:16-:18 (1986); New Jersey, *see* N.J. STAT. ANN. §§ 2A:38A-1 to -6, 2C:20-23 to -32 (West 1987 & Supp. 1992); New Mexico, *see* N.M. STAT. ANN. §§ 30-45-1 to -7 (Michie Supp. 1989); North Carolina, *see* N.C. GEN. STAT. §§ 14-453 to -457 (1992); North Dakota, *see* N.D. CENT. CODE § 12.1-06 to 08 (Supp. 1993); Ohio, *see* OHIO REV. CODE ANN. § 2913.04 (Baldwin 1992); Oklahoma, *see* OKLA. STAT. ANN. tit. 21, §§ 1951-1958 (West Supp. 1993); Oregon, *see* OR. REV. STAT. § 164.377 (1990); Pennsylvania, *see* 18 PA. CONS. STAT. ANN. § 3933 (Supp. 1993); Rhode Island, *see* R.I. GEN. LAWS §§ 11-52-1 to -8 (1981 & Supp. 1992); South Carolina, *see* S.C. CODE ANN. §§ 16-16-10 to -40 (Law. Co-op. 1985); South Dakota, *see* S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to -8 (1986 & Supp. 1993); Tennessee, *see* TENN. CODE ANN. §§ 39-14-601 to -603 (1991); Utah, *see* UTAH CODE ANN. §§ 76-6-701 to -705 (1988 & Supp. 1993); Virginia, *see* VA. CODE ANN. §§ 18.2-152.1 to .14 (Michie 1988 & Supp. 1993); West Virginia, *see* W. VA. CODE §§ 61-3C-1 to -21 (1992); and Wisconsin, *see* WIS. STAT. ANN. § 943.70 (West Supp. 1992).

143. *See supra* notes 125-28 and accompanying text and *infra* notes 195-205 and accompanying text.

144. States that have taken this approach include: California, *see* CAL. PENAL CODE §§ 502(e)(1) (West 1988 & Supp. 1993); Illinois, *see* ILL. ANN. STAT. ch. 38, para. 16D-3(3)-(4) (Smith-Hurd Supp. 1992); Maine, *see* ME. REV. STAT. ANN. tit. 17A, § 433(1)(B), (C) (West Supp. 1992); Minnesota, *see* MINN. STAT. ANN. § 609.88 (West 1987 & Supp. 1993); New York, *see* N.Y. PENAL LAW §§ 156.20-156.27 (McKinney 1988 & Supp. 1993); and Texas, *see* TEX. PENAL CODE ANN. §§ 33.01-.04 (West 1989 & Supp. 1992).

145. *See* MINN. STAT. ANN. § 609.88(1)(c) (West Supp. 1993).

146. *See id.* § 609.87(12).

operating under such statutes still lack the ability to prosecute a programmer who creates an "enabler"—a device that is not malevolent software per se, but is a package that allows another party to create malevolent software.[147]

III. THE JUDICIAL SYSTEM'S RESPONSE TO MALEVOLENT SOFTWARE

A. Federal Cases

Although *Sawyer v. Department of Air Force*[148] marked the commencement of computer crime prosecution, *United States v. Morris*[149] remains the only successful prosecution under the CFAA following its amendment in 1986.[150] Although the Second Circuit upheld Morris' conviction, his defense illuminated the problems inherent within the CFAA.[151]

Morris received authorization to use university computers connected to the Internet computer network while enrolled in the Cornell University computer science Ph.D. program.[152] After familiarizing himself with the security measures employed on the network, he concluded that they were inadequate.[153] To demonstrate this, Morris developed and released a worm[154] on the Internet.[155] Although the worm was designed to exploit several security defects Morris discovered, Morris did not intend the worm to interfere with normal computer usage.[156] Unfortunately his calcula-

147. Recently, a malevolent software creator known as the "Dark Avenger" posted copies of his virus development kit on several computer bulletin boards, making them freely available for public download and use. Lance Ulanoff, *Virus Spread: Who's to Blame*, PC MAG., Oct. 13, 1992, at 31. "Enabler" software gives those with no knowledge of programming the ability to create malevolent software capable of destroying or damaging computers and information contained therein. *Virus Hackers and Information War*, UPI, Sept. 14, 1992, *available in* LEXIS, Nexis Library, UPI File. In this same context, the question arises whether the author of a book may be prosecuted for providing source code for malevolent software. Mark Ludwig's *Little Black Book of Computer Viruses* is just such a book. It is available at bookstores for $15 and is referred to as a "cookbook for virus writers." Bill Husted, *Business Report: On Technology*, ATLANTA J. & CONST., Oct. 8, 1992, at G2.

148. 31 M.S.P.B. 193 (July 9, 1986).

149. 928 F.2d 504 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991).

150. Michael Alexander, *Morris Case Centers on Intent*, COMPUTERWORLD, Jan. 15, 1990, at 6.

151. *See infra* notes 160-69 and accompanying text.

152. 928 F.2d at 505.

153. *Id.*

154. *See supra* note 10 and accompanying text.

155. 928 F.2d at 505. The worm was released on November 2, 1988, from a computer housed at the Massachusetts Institute of Technology. *Id.* at 506. Morris selected MIT as the transmission point to divert attention away from Cornell, where he had developed the worm. *Id.*

156. *Id.* at 505.

tions were flawed and the worm paralyzed computers at locations throughout the network.[157] The costs of removing the worm from each infected location ranged from "$200 to more than $53,000."[158] A jury convicted Morris of violating the CFAA, sentenced him to three years of probation, 400 hours of community service, and ordered him to pay a $10,050 fine as well as the costs of his supervision.[159]

Morris' appeal to the Second Circuit raised two issues. First, does the intent element of section (a)(5)(A) of the CFAA[160] modify *both* the requirement of accessing a federal interest computer and preventing authorized use that results in a loss, or does the intent element modify only the access requirement? Second, what must be established to prove that "access without authorization" occurred under the CFAA?[161]

Morris first argued that the specific language of section (a)(5)(A)[162] indicates that the intent element modifies both clauses.[163] According to Morris, he intended to access a federal interest computer, but did not intend to prevent authorized use and a resulting loss.[164] In response, the Government argued that the intent element modifies only accessing a

---

157. *Id.* at 506. After Morris realized his "miscalculations," he and a friend developed a vaccine to kill the worm and sent out an anonymous message on the Internet network providing the so-called cure. *Id.* However, Morris' worm had so completely fouled the network that the message containing the vaccine did not reach other users quickly enough to allow them to protect computers not yet infected. *Id.*

158. *Id.*

159. *Id.* Morris was found to have violated section (a)(5)(A) of the CFAA. *Id.* *See supra* note 108 and accompanying text.

160. Section (a)(5) of the CFAA begins with the language, "intentionally accesses," 18 U.S.C. § 1030(a)(5) (Supp. I 1992), and is followed by two requirements that constitute a violation of this section. *See infra* note 162.

161. 928 F.2d at 505.

162. The precise language of Section (a)(5)(A) states:

> (a)(5) Whoever—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 . . . .

18 U.S.C. § 1030(a)(5)(A) (Supp. I 1992).

163. Morris' argument was that the "intended to" language modified both clauses of section (a)(5). 928 F.2d at 507. Morris cited the Senate and House reports on the CFAA, pointing to "the careful attention that Congress gave to selecting the scienter requirement" for this section. *Id.* at 508. The *Senate Report* indicates that the intent requirement of section (a)(5) was designed to "penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another." *Id.* (citing S. REP. NO. 432, *supra* note 97, at 5, 10, *reprinted in* 1986 U.S.C.C.A.N. at 2483, 2488).

164. 928 F.2d at 508.

federal interest computer, claiming that intent to prevent authorized access and cause a loss need not be established.[165] The court found the Government's argument persuasive and held that the scienter element applies only to the access requirement of section (a)(5)(A) of the CFAA.[166]

Morris also contended that by placing the worm on the Internet, he had exceeded his "authorized access," but had not engaged in an act of "unauthorized access."[167] Cognizant of Morris' authorization to use computers connected to the Internet,[168] the court found that Morris had used the computers for other than authorized purposes and rejected this argument.[169] The portion of the decision addressing Morris' access remains the most troublesome aspect of the opinion. The court refused to base its finding of unauthorized access on Morris' insertion of the worm and suggested that his activities, other than the use of unauthorized services and features on network computers, may have been authorized.[170] Rather than seizing the opportunity to provide guidance in the interpretation of the CFAA, the court authored a very fact-specific opinion that has limited value as precedent. Even worse, the opinion leaves open the possibility of authorized malevolent software within the confines of the CFAA.[171]

B. State Cases

State prosecution of malevolent software creators occurs infrequently. Not only does most state legislation suffer from the same shortcomings as the CFAA, but a large percentage of computer crimes are interstate in

---

165. *Id.* at 508-09. The Government relied upon the changes made in the 1986 amendments to the CFAA. *Id.* at 508. Specifically, they compared the current section (a)(5) with its predecessor, which placed a mental state requirement before both the "access" phrase and "damage" phrase. *Id.* The Government's argument centered on the failure of section (a)(5) to place a scienter requirement before both clauses. Therefore the Government argued that this clearly indicates that Congress intended to apply the scienter requirement to only the clause governing "access". *Id.* (citing S. REP. NO. 432, *supra* note 97, at 5-6, *reprinted in* 1986 U.S.C.C.A.N. at 2482-83).

166. *Id.* at 509.

167. *Id.* This was Morris' second attempt to slip from the grasp of section (a)(5) using an argument based on statutory construction. Morris' argument focused on the language of the associated *Senate Report*, which stated that section (a)(5) was aimed at those who lacked authorization to access any federal interest computer. *Id.* at 510 (citing S. REP. NO. 432, *supra* note 97, at 5, 10, *reprinted in* 1986 U.S.C.C.A.N. at 2483, 2488).

168. *Id.*

169. *Id.* Specifically, the court pointed to his use of the computers on the network to find holes in the operating software that permitted him to gain unauthorized access to other computers. *Id.*

170. *Id.*

171. *See, e.g.*, S. REP. NO. 544, *supra* note 95, at 5.

nature and the federal government typically has greater resources to devote to investigation and prosecution.[172]

The first successful state prosecution of a malevolent software creator did not occur until 1991. That case, *Burleson v. State*,[173] arose from the insertion of malevolent software in a company computer that resulted in the destruction of payroll data.[174] Shortly after Burleson was fired, someone accessed his computer terminal using his password and security clearance.[175] Computer logs indicated that actions taken during the unauthorized access triggered malevolent software responsible for destroying the data.[176] A jury convicted Burleson of harmful access to a computer, sentenced him to seven years probation, and ordered him to pay $11,800 in restitution.[177]

Werner, Zaroff, Slotnick, Stern & Askenazy v. Lewis[178] involved insurance claim tracking software that abruptly ceased operation when it reached the 56,789th claim.[179] Lewis had modified and installed software designed to automate the administrative portion of plaintiff's insurance claim litigation.[180] A software consultant hired by plaintiff to correct the problem discovered that a conditional statement, similar to a logic bomb,[181] placed in the source code had forced the software to malfunc-

---

172. Stephen Fishbein, *What Victims of Computer Crime Should Know and Do*, N.Y.L.J., Nov. 12, 1993, at 4.

173. 802 S.W.2d 429 (Tex. Ct. App. 1991).

174. *Id.* at 433. Evidence presented at trial indicated that shortly after Burleson was fired, a large number of records needed to compile the monthly payroll commission report were reported missing from the company's computer system. *Id.* USPA employed approximately 450 agents worldwide that were paid monthly commissions totalling approximately $2 million. *Id.* Commissions were calculated by compiling information gathered from numerous sources on the company's computer system. *Id.*

175. *Id.* Testimony at trial suggested that even though Burleson turned in his set of keys upon dismissal, he retained at least one extra key to the building. *Id.*

176. *Id.* at 433-34.

177. *Id.* at 432.

178. 588 N.Y.S.2d 960 (N.Y. Civ. Ct. 1992).

179. *Id.* at 961. When the system shut down, plaintiff was unable to use its computer system for claims or billing purposes. *Id.* Although the system could have been restarted by creating an additional sub-directory to store files, plaintiff did not know this. *Id.*

180. *Id.* at 960. Upon receipt of the final payment for his services, Lewis had inserted a disk into plaintiff's computer and indicated that had he not been paid, he would not have loaded the data contained on the floppy disk into the computer. *Id.* He claimed that the data on the disk was vital to the proper functioning of the software he installed. *Id.* Curiously, Lewis telephoned plaintiff's offices on a monthly basis to determine how many claims had been entered into the computer. *Id.* at 960-61. Although Lewis denied the allegations, the court gave his statements little respect in light of the inherently suspicious nature of the number 56,789. *Id.* at 961.

181. *See supra* note 11 and accompanying text.

tion.[182] A jury convicted Lewis of computer tampering and awarded plaintiff punitive damages of $18,000 and compensatory damages of $7,000.[183]

More recently, James Joseph Welsh pleaded guilty to destroying files on his former wife's computer using a trojan horse.[184] Although he could have received a three year state prison term, Welsh received a four month sentence and was ordered to pay $12,000 in restitution and spend 300 hours teaching high school computer science classes.[185]

IV. CRITICISM OF CURRENT LEGISLATION

Although federal[186] and state[187] laws address computer crime, most of the legislation was enacted during the period of 1984-1988.[188] Technological innovation[189] and wide scale acceptance of the personal computer have dramatically changed the regulatory needs in this area.[190] During this period of dynamic technological change, however, the regulatory environment has remained static. Malevolent software, born during this period of legislative inactivity, has proliferated and cannot be considered only a short-term problem. Malevolent software creators have developed over 1,200 strains of malevolent software,[191] and have organized into groups to promote proliferation.[192] Unfortunately, these

---

182. 588 N.Y.S.2d at 961. The consultant testified at trial that, in his opinion, the software had ceased to function because of a conditional statement added to the programming code by Lewis, the individual responsible for the original modification and installation of the software. *Id.*

183. *Id.* at 963.

184. *Computer Hacker Gets 4 Months in Jail*, S.F. CHRON., Aug. 18, 1993, at A12. Welsh's former wife had been having problems with her computer and she called him seeking a solution. Ron Sonenshine, *Hacker Denies Ruining Computer Files: Virus Allegedly Destroyed System of His Ex-Wife*, S.F. CHRON., Dec. 3, 1992, at A21. He volunteered to send her a disk that would correct her problems which she gladly accepted. *Id.* After placing the disk in her computer, the screen filled with zeros and twenty minutes later a limerick appeared on her screen. *Id.* It read: "A lying bitch named Kathleen made in the courts quite a scene, To have her ex, the hacker, Enjoined not to smack her, So I wiped her whole hard disk clean." *Id.* Welsh's wife had claimed during divorce proceedings that he had beaten her. *Id.* The trojan horse allegedly reformatted her computer's hard disk after displaying the limerick, causing her to lose data from two previous books as well as several years of tax material. *Id.*

185. *See Computer Hacker Gets 4 Months in Jail*, *supra* note 184 at A12.

186. *See supra* part II.A.

187. *See supra* part II.B.

188. *See supra* notes 135, 138, 142. *But see supra* note 144.

189. *See* Seymour, *supra* note 6, at 193-94.

190. *See generally* Clark, *supra* note 7.

191. *See* Lateulere, *supra* note 19, at 105.

192. *See supra* notes 15-16 and accompanying text.

hackers show no signs of halting their efforts.[193] Most computer experts no longer ponder the possibility of infection but consider how soon it will occur and how to respond.[194] A problem of this magnitude must receive proper legislative treatment.

A practitioner attempting to apply the CFAA first encounters difficulty in determining the exact scope of the legislation. Does the CFAA actually apply to many of today's computers? Section (e)(1) defines "computer" to exclude automated typesetters, hand calculators and similar devices. This distinction threatens to exclude laptop and palmtop computers[195] and computers utilized in desktop publishing or printing applications from protection under the CFAA.[196] Furthermore, most of the activities proscribed by the CFAA relate to the destruction or alteration of "information."[197] Failure to define this critical term leaves unanswered the question whether data currently in RAM is protected or whether only data placed on a physical storage medium is covered.[198]

"Unauthorized access" is a central element in all causes of action under the CFAA,[199] yet lack of a defining provision or expression of legislative intent leaves the precise meaning of the term unclear. Furthermore, while prohibitions on accessing computers may have been sufficient in 1986, they fail clearly to criminalize the placement of malevolent software in apparently legitimate software products[200] or other data files that authorized users subsequently place on their computers or networks.[201] The transmission of malevolent software does not require its creator to "access"

---

193. Hackers have even begun holding meetings and conventions. *See* Flanagan & McMenamin, *supra* note 46, at 188. Six cities in the United States host meetings organized by the publishers of *2600* on the first Friday of every month. *See* Didio, *supra* note 14, at 72. These meetings allow readers to submit articles for publication and ask questions. *Id.* A side benefit is the chance to visually identify the undercover agents who follow computer criminals as they often show up to observe and take note. *Id. See generally* BRUCE STERLING, THE HACKER CRACKDOWN (1992) (describing the extensive nature of computer crime, its continued increase over the past decade and the threat it poses to society).

194. "These days, computer viruses are a fact of life. Users are faced with three choices: run scared and stop sharing, get tough and install a lot of viral protection packages, or use common sense and practice good computer hygiene." *See* DiDio, *supra* note 14, at 73.

195. *See supra* note 127.

196. Even if a computer falls within these guidelines, it must also be a federal interest computer to be covered by the CFAA. *See supra* note 102 and accompanying text.

197. *See, e.g.*, 18 U.S.C. §§ 1030(a)(1), (a)(2), (a)(5), (a)(6) (Supp. I 1992).

198. Physical storage mediums include a hard or floppy disk, floptical disk or data tape.

199. *See supra* note 115 and accompanying text.

200. *See* Charnet, *supra* note 99, at 33.

201. *Id.*

every computer that is infected.[202] This focus also ignores the possibility that an authorized user could engage in destructive actions.[203] Finally, the current statute effectively forecloses prosecution of someone who creates an enabler[204] or authors a book that provides source code for malevolent software.[205]

Criminalization of the unknowing transmission of malevolent software is undesirable.[206] Successful prosecution of malevolent software creators will, however, continue to hinge upon judicial interpretation of ambiguous terms such as "computer,"[207] "information,"[208] and "access."[209] Another determining factor will be whether courts employ inventive applications of the CFAA to malevolent software creators, as illustrated by the *Morris* case.[210] Until the CFAA is amended to reflect changes in the nature of computer crime, the difficulty of successfully prosecuting a malevolent software creator will remain high.[211]

A review of the CFAA's sentencing guidelines also must be undertaken. Conviction carries a maximum penalty of a fine and imprisonment for no more than ten years.[212] In certain instances, imprisonment may be limited to no more than one year.[213] These penalties might deter individuals from engaging in conduct that carried with it a high probability of detection.[214] Those responsible for the creation and transmission of malevolent software

---

202. *See supra* part I.B.

203. Can a "hospital employee who inserts a virus into a computer and destroys thousands of patient records be immune from prosecution because he had the authority to access the computer?" *See* Charnet, *supra* note 99, at 33.

204. *See supra* note 147 and accompanying text.

205. *See generally* Husted, *supra* note 147.

206. Even legislation proscribing the creation and transmission of malevolent software will not completely eliminate this problem. Consequently, computer users will still need adequate protective devices. Even if legitimate research regarding malevolent software is prohibited, commercial protection devices will fall behind those creating the malevolent software. Furthermore, many computer scientists are considering the possible use of viruses or worms to perform beneficial activities. *See* Markoff, *supra* note 120. One researcher has even offered a $1,000 annual prize for the most useful computer virus submitted to him. *Id.* Many computer security experts, however, oppose this. One likened it to giving an award for someone who comes up with the "best use for a handgun." *Id.*

207. *See supra* notes 126-27 and accompanying text.

208. *See supra* note 128 and accompanying text.

209. *See supra* note 115 and accompanying text.

210. *See supra* part III.A.

211. *See, e.g.*, Flanagan & McMenamin, *supra* note 46, at 184.

212. This sentence applies to first time offenders. *See* 18 U.S.C. § 1030(C) (Supp. I 1992).

213. *See id.* § 1030(C)(2)(A).

214. Very few malevolent software creators are ever apprehended. *See, e.g.*, Flanagan & McMenamin, *supra* note 46, at 186.

are, however, rarely apprehended.[215] The sentencing guidelines also fall short when addressing recidivists. Those previously convicted under the CFAA face enhanced punishment only under limited circumstances.[216]

Adding to the ineffectiveness of the CFAA and its progeny is the fact that federal and state courts have been reluctant to impose prison sentences upon those successfully prosecuted.[217] The 1990 attack on the Harvard-Smithsonian Astronomical Observatory via the Internet,[218] masterminded by a malevolent software creator seeking personal retribution against a virus researcher, illustrates the result of this judicial leniency.

Congressional amendment of the CFAA and federal pressure on state legislatures to follow suit offer a solution to these problems. This method would, however, perpetuate the "federal interest" computer distinction drawn by the CFAA,[219] a standard no longer appropriate due to increasing numbers of modems,[220] computer bulletin board systems,[221] and the large-scale use of computer networks in both the public and private sector.[222] A modem enables a single, previously isolated computer to connect and exchange data with any other similarly equipped computer or network in the world using a standard telephone line.[223] While data may be the desired item of exchange, malevolent software may be an unknown passenger as well.[224] The increase in the networking of personal computers means that a single piece of malevolent software, residing on one personal computer, can infect computers throughout the world.[225]

---

215. *Id.*

216. *See supra* note 112 and accompanying text.

217. *See supra* notes 159, 177, 183, 185 and accompanying text.

218. *See supra* notes 46-47 and accompanying text.

219. *See supra* note 102 and accompanying text.

220. A modem is a device used to transmit computer data over telephone lines. WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 762 (9th ed. 1986). Computer manufacturers can buy 2,400 baud modems with send and receive fax capability for $19. John C. Dvorak, *Inside Track*, PC MAG., Feb. 23, 1993, at 95.

221. *See supra* note 27 (describing numerous uses for computer bulletin board systems, their growing popularity and ability to link interstate computer users).

222. *See Computer Viruses: New Research Shows Epidemic Proportions*, *supra* note 26. Even the State of New York has implemented a large computer network, Empire Net, to link over 8,000 state agency computers in an effort to cut costs. Bob Brown, *States Take Steps to Crack Down on Network Hackers: Legislation Aimed at Preventing Net Virus Attacks*, NETWORK WORLD, July 17, 1989, at 8.

223. *See supra* note 220.

224. *See supra* notes 26-28 and accompanying text.

225. For example, a user whose computer was infected could connect to an international network such as the Internet and upload a file onto the network that contained a strain of malevolent software. If the software was not detected by a scanning system, *see supra* note 81, on the host computer, infection could spread throughout the Internet through this simple exchange of data. *See, e.g.*, United

Individual computers can no longer be considered as autonomous units, provided with segmented protection dependent upon their particular use or location.

New statutes or amendments to the CFAA directed at malevolent software should move towards federal occupation of this area,[226] providing a regulatory approach that characterizes individual computers as nodes on a large, nation-wide network. Even stand alone computers that are neither connected to a network nor have a modem can be the source of a nation-wide infection if an infected disk from the computer is introduced to another networked computer. Conscious of the limitations of the Commerce Clause,[227] the drafters of the CFAA chose to allow states to protect their own intrastate computer users.[228] However, even intrastate computer usage now has the potential to affect interstate commerce.[229]

The Computer Abuse Amendments Act of 1992 (CAAA) is the solution currently being considered at the federal level.[230] The CAAA was focused primarily upon realigning section (a)(5) of the CFAA, and has attempted to codify three offenses relating to the transmission of malevolent software. The CAAA would make it a felony to employ a computer used in interstate

---

States v. Morris, 928 F.2d 504, 506 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991).

226. The author is suggesting that inclusive federal legislation be enacted, eliminating the need for parallel state legislation applicable to computers unable to meet the Federal interest distinction. *See supra* note 102 and accompanying text.

227. U.S. CONST. art. I, § 8.

228. *See supra* note 129.

229. The author is suggesting that federal occupation of the computer crime arena would not violate the limitations imposed upon the federal government by the Commerce Clause. In Wickard v. Filburn, 317 U.S. 111 (1942), the Supreme Court articulated the "cumulative effect" theory, allowing the expansion of Commerce Clause powers to regulate an entire class of acts, if the class has a substantial economic impact on interstate commerce. This extension was found to be within the confines of Commerce Clause power even if one act alone, within the class, would have little if any impact on interstate commerce.

This doctrine was applied in Perez v. U.S., 402 U.S. 146 (1971), to uphold the loan-sharking provisions of the Consumer Credit Protection Act as applied to transactions occurring within the confines of one state. The Court found it persuasive that loansharking as a whole, affected interstate commerce. *Id.* at 151-52.

Under this reading of Commerce Clause powers, federal occupation of the computer crime arena, a class of activities that substantially affects interstate commerce as a whole, would not be unconstitutional.

230. This Act was introduced as an amendment to H.R. 3349. 138 CONG. REC. S17,802-01, S17,806 (daily ed. Oct. 8, 1992) (statement of Sen. Leahy). The Act would amend the CFAA and take into consideration testimony and research that has been carried out since 1989 regarding the proliferation of malevolent software and the threat it poses. *Id.*

commerce or communications[231] to: (1) knowingly transmit a program, code, information or instructions with the intent to (a) damage a computer or computer system or (b) effectively withhold the use of a computer or computer system;[232] or (2) knowingly transmit the harmful portion of a program, code, information or instructions without the permission or knowledge of those responsible for the computer or computer system that receives this transmission.[233] Furthermore, the CAAA makes it a misdemeanor knowingly to transmit a program, code, information or instructions through the use of a computer used in interstate commerce or communication with reckless disregard of the unjustifiable risk that such results will follow.[234] The CAAA also creates civil remedies in the case of any felony violation under the CFAA.[235]

Although the CAAA provides an innovative response to malevolent software, it too suffers from an inappropriate focus and suspect distinctions.[236] The new prohibitions created by the CAAA focus on "transmission." While it is true that malevolent software creators transmit the fruits of their labors, this act may only occur once. The infection typically spreads when other users unknowingly transmit infected files.[237] The creation of a misdemeanor provision, although a sound idea, falls victim to poor implementation. By establishing "recklessness," borrowed from the

---

231. The CAAA modifies the federal interest computer distinction, *see supra* note 93 and accompanying text, and adds a further twist by including computers engaged in interstate communication. *See generally* 136 CONG. REC. S18,233-01 (1990).

232. S. 1322, 102d Cong., 1st Sess. § (a)(5)(A)(i) (1991). This newly-created offense would remain in the same classification as the prior section (a)(5) for sentencing purposes. *See supra* note 111.

233. S. 1322, 102d Cong., 1st Sess. § (a)(5)(A)(ii) (1991). In addition, this transmission must: (1) cause a loss aggregating $1,000 or more during a single year; or (2) impair or modify (or have the propensity to do so), the medical care or treatment of one or more individuals. *Id.* § (a)(5)(A)(ii)(II). These additional requirements are taken verbatim from sections (a)(5)(A) and (a)(5)(B) of the CFAA. *See supra* note 108. This newly-created offense would remain in the same classification as the prior section (a)(5) for sentencing purposes. *See supra* note 111.

234. Violation of the misdemeanor provisions of the CAAA occurs under the same circumstances as a violation of the felony provisions. *See supra* notes 232-33 and accompanying text. Only the mens rea element is altered. *See* S. 1322, 102d Cong., 1st Sess. § (a)(5)(B)(i) (1991). The penalty under this provision is a fine or imprisonment for not more than 1 year or both. *Id.* § (c)(4).

235. *Id.* § (g). Only compensatory damages and injunctive or other equitable relief is available. *Id.* If the violation does not relate to the impairment or potential impairment of medical treatment or diagnosis, *see supra* note 233, only economic damages may be recovered. S. 1322, 102d Cong., 1st Sess. § (g) (1991).

236. *See supra* notes 113-128 and accompanying text.

237. *See supra* notes 25-28 and accompanying text. This means that successful prosecution would require the infection to be traced back to the initial transmission performed by the malevolent software creator.

Model Penal Code,[238] as the required mental state, the CAAA would permit an individual to disregard known consequences of transmitting malevolent software and escape with only a misdemeanor conviction. Furthermore, the fine line between knowing[239] and reckless transmission would be frequently contested because of the respective penalties.

V. PROPOSAL

The proper response to the growing problem of malevolent software can be implemented as a four part amendment to the CFAA. First, the federal interest computer distinction should be abandoned in favor of a comprehensive provision that extends protection to all computers within the United States. Second, the focus of section (a)(5) of the CFAA must be shifted from accessing a computer to creating and transmitting any form of malevolent software. Specifically, malevolent software creators should be held liable for damage that occurs on any computers they access and transmit malevolent software to, as well as computers subsequently infected as a result of the initial infection or transmission. This standard should apply regardless of whether the creator was involved with, or intended the subsequent transmission or infection. This realignment would broaden the category of individuals and conduct covered by the CFAA while providing flexibility in prosecution. Third, the class of information protected should be clarified and expanded to include information in RAM as well as that stored on physical mediums. Finally, sentencing guidelines for first-time offenders and recidivists must be strengthened. Not only should prison terms be increased, but confiscation of computer hardware and software used in the creation or transmission of malevolent software should also be permissible.[240] Stringent guidelines deter would-be creators and notify the judiciary that such individuals are to be punished. Until such comprehensive measures are undertaken, make sure your vaccines are up to date[241] or risk an infection!

Bradley S. Davis

---

238. *See* MODEL PENAL CODE § 2.02(2)(c) (Official Draft 1985).

239. *See id.* § 2.02(2)(b).

240. Several states have already included provisions that allow for confiscation of computer equipment when a violation of a computer crime statute has occurred. *See, e.g.*, N.M. STAT. ANN. § 30-45-7 (Michie Supp. 1989); CAL. PENAL CODE § 502.01 (West Supp. 1993).

241. *See supra* notes 83-84 and accompanying text.