Fall 1993


Joseph P. Daly

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

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

Recommended Citation

COMMENTS

THE COMPUTER FRAUD AND ABUSE ACT—A NEW PERSPECTIVE: LET THE PUNISHMENT FIT THE DAMAGE

I. INTRODUCTION

At age 24, Robert Tappan Morris, was pursuing his graduate degree in computer studies at Cornell University.1 Morris boasted an impressive background in computer programming, including undergraduate work at Harvard University,² and he seemed destined for a successful and perhaps lucrative career in computer science. One area which particularly intrigued Morris was computer security and how it could be circumvented.³ Consequently, Morris decided to work on a computer program that would illustrate the ease with which he could breach a computer system.⁴ Morris’ program not only succeeded, but thrust him into the national spotlight. In United States v. Morris,⁵ the United States Court of Appeals for the Second Circuit heard the first criminal prosecution of a computer virus crime under the Computer Fraud and Abuse Act of 1986 (“the Act”).⁶

The method Morris chose to demonstrate the inadequacies of a computer system was to release a computer “worm”⁷ into the IN-

---

2. Id.
3. Morris’ interests are not surprising in light of his father’s work in the field of computers. Robert T. Morris, Sr., at the time of his son’s trial, was the chief scientist at the National Computer Security Center and, interestingly enough, was one of the original designers of a computer virus game called “Core War.” Anne Branscomb, Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, 16 Rutgers Computer & Tech. L.J. 1, n. 42 (1990). “Core War” players try to design computer virus programs that will replicate themselves onto other programs before viruses created by other players seek them out and destroy them. Id. The player whose virus is the sole survivor “wins.” Id.
4. Morris, 928 F.2d at 505.
5. Id. at 504.
7. A computer “worm” is a special type of virus program that is designed to move from computer to computer through a computer network. Daniel J. Kluth, The Computer
TERNET\textsuperscript{8} computer network,\textsuperscript{9} which links an estimated 60,000 scientific, academic, and governmental computers\textsuperscript{10} around the world. Morris programmed the worm to spread throughout the INTERNET system so that anyone who linked onto it would become infected.\textsuperscript{11} The worm would then force the infected computer to perform extraneous calculations until it became temporarily inoperable.\textsuperscript{12}

Morris went to great lengths to ensure that he would not be de-

Beneficially, it can help to locate idle computers for authorized users in a network. \textit{Id.}
When the worm is destructive, as most are, it moves through the network disabling computers by filling up the memory, freezing the keyboards and screens, or slowing down the computer's execution time. \textit{Id.}
Unlike a simple virus, a worm does not attach itself to any computer in the system, but rather infects them as it moves throughout the system. \textit{Id.}

8. INTERNET is a computer “network of networks” that serves as the primary network for research facilities in the United States. Phillip Elmer-DeWitt, \textit{The Kid Put Us Out of Action}, Time, Nov. 14, 1988, at 76. It is comprised of over 500 unclassified networks across the country. \textit{Id.}
Among the institutions whose systems link to INTERNET are: NASA, the Massachusetts Institute of Technology, University of California at Berkeley and San Diego, the Rand Corporation, the Los Alamos National Laboratory, Johns Hopkins University at Baltimore, and the United States Logistics Command at Wright Patterson Air Force Base. \textit{Id.}

9. A computer network is a system which “makes available to a data processing user at one place some data processing function or service performed at another place.” Hugh Green, \textit{The Structure of Computer Networks, Computer Network Architectures and Protocols} 3 (P.E. Green ed. 1982). A network can be a simple link between a few small terminals, to a system linking hundreds of processing units of various sizes, which are interconnected to each other and simultaneously to tens of thousands of other terminals. \textit{Id.}

10. Two of the many networks in INTERNET links are ARPANET and MILNET, both unclassified military networks. See Branscomb, \textit{supra} note 3. ARPANET is a network created by the Defense Advance Research Projects Agency (DARPA), and is intended for academic use. \textit{Id.} MILNET is an unclassified network of the Department of Defense. \textit{Id.}

11. Morris formulated four ways that the virus could be spread: 1) through an error, or “bug” in the computer mail program that allows one system to receive mail electronically from another computer; 2) through a “finger demon” program that makes available limited information on other users; 3) through the “trusted host” program that allows a user with authorization on one system to gain authorization on another system without requiring a password; and 4) through a program of password-guessing, that performs random combinations of passwords until access is gained. United States v. Morris, 928 F.2d 504, 506 (2d Cir. 1991).

12. Morris designed the virus to draw as little attention to itself as possible by making it very difficult to detect, and thus more difficult to “kill.” \textit{Id.} at 505. He programmed the virus to only spread to computers which were not yet infected, because the virus would be more readily identified if it were allowed to copy itself more than once onto the same computer. \textit{Id.} In essence, the worm would “ask” a computer if it had the virus yet, and if it responded “no,” then it would infect that computer. \textit{Id.}
Realizing that a programmer could easily pre-program his computer to respond affirmatively to such a request and thus avoid infection, Morris instructed the worm to copy itself every seventh time it received a
tected. Unfortunately, a mathematical error dashed Morris' hopes for anonymity. The error caused the worm to spread far more quickly and widely than he had anticipated. Thus, all across the country, computers linked to INTERNET either overloaded or shut down completely. Morris attempted to rectify his conduct by anonymously sending messages through the system which contained instructions on how to kill the virus, but countless millions of dollars in damage had already occurred.

The District Court for the Northern District of New York convicted Morris of violating the Computer Fraud and Abuse Act and sentenced him to three years of probation, 400 hours of community service, and fined him $10,050 plus court costs. On appeal, the United States Court of Appeals for the Second Circuit affirmed the conviction.

This Comment argues that Morris' grossly lenient sentence is symptomatic of a greater problem—the inadequate sentencing scheme of the Computer Fraud and Abuse Act. First, this Comment will examine computer viruses in general and the Computer Fraud and Abuse Act.
Act. Second, this Comment will propose the implementation of a sentencing scheme by which individual sentences would be allocated according to the damages caused by a computer virus propagator.\textsuperscript{20} Third, this Comment will illustrate the utility of such a scheme in both current criminal and civil law. Fourth, this Comment will discuss potential methods of quantifying computer virus damages. Finally, this Comment will conclude that the Computer Fraud and Abuse Act, while a potentially effective tool for prosecuting people who design and spread computer viruses, needs to be amended in order to set punishments which correspond with the damages caused by each particular virus.

II. A SURVEY OF THE COMPUTER VIRUS

Our society, both global and national, relies heavily on computers in countless aspects of its daily operation.\textsuperscript{21} Whether we realize it or not, each day our lives are monitored, altered, and even preserved by computers. On a large-scale level, computers monitor our national defense and guard against enemy attack,\textsuperscript{22} and on a smaller scale, computers are integral factors in maintaining health care,\textsuperscript{23} financial services,\textsuperscript{24} and businesses.\textsuperscript{25} The reliance we place on computers is such that devastating results occur when certain computers malfunction.\textsuperscript{26}

Unfortunately, most people fail to appreciate the utility and value of computers until one malfunctions. As harrowing an experience as

\textsuperscript{20} In the area of computer crime, the programmer of a computer virus is also known as a "propagator." See Kluth, \textit{supra} note 7, at 297.


\textsuperscript{23} On an administrative level, hospitals rely on computers to maintain and update patient information, as well as for billing purposes. \textit{The Washington Post}, Mar. 23, 1989, at A5. In addition to these functions, computers also play integral roles in medical analysis and in creating high-quality pictures for diagnosing diseases. \textit{Id}.

\textsuperscript{24} There are four major electronic funds-transfer networks in the United States that alone carry "the equivalent of the federal budget every two or four hours." \textit{See Branscomb, \textit{supra} note 3, at n.4.}

\textsuperscript{25} \textit{Id.} at n.3.

\textsuperscript{26} One such catastrophic effect was when a computer malfunction resulted in the deaths of at least three patients after an error occurred in a computer software-controlled radiation therapy machine. Harry F. Rosenthal, \textit{Computer Security Is Too Flimsy}, \textit{Phoenix Gazette}, Dec. 10, 1990, at B5.
this may be, despair turns to frustration when the source of a computer's malfunction is a destructive computer virus, which has been carefully calculated, designed, and released by a "hacker,"motivated solely by destruction for its own sake. Essentially, these "hackers" are committing high-tech vandalism. Fortunately, public awareness of computer viruses is growing, due in part to both the growing dependence on computers, and also to the increasing publicity surrounding recent viruses such as "Michaelangelo" and "Jerusalem", both of

27. For the purposes of this Comment, a computer virus is a computer program containing instructions that attaches itself to other programs or computer systems through any one of a number of means. See Marion, supra note 14, at 627. Once inside a program, the instructions may repeat over and over until all other programs in the system have been "infected" with these instructions. Id. The effect of these instructions is usually a system overload which forces the contaminated system to perform endless tasks until the overload occurs, thus shutting down the entire system. Files may also be erased, erroneous information inserted, and equipment destroyed. Id. Federal courts adopted the following definition of computer virus: "a migrating program which attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer." United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

Although the majority of viruses effect adverse results, one should note that there are certain viruses which may not be so malignant, and are therefore termed "benign." See Kluth, supra note 7, at n.15 (discussing benign viruses). Even so-called "benign" viruses may be costly and destructive in that they occupy computer execution time, and require the costly services of expert programmers to locate and remove them from the system. Id. Benign viruses are the minority, however, and as referred to in this Comment, computer viruses will be considered to be of the malignant variety.


28. The definitions of "hacker" are nearly as numerous as the viruses which they create. The most generic (and kind) definition of a "hacker" is "a person who is not trying to learn about computers in a meaningful manner, but rather through trial and error." WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS 168 (3rd ed. 1988). More specifically, a "hacker" is considered one who interferes with computer programs. Brian McConnell, Global Warning, NEW LAW JOURNAL, Mar. 2, 1990, at 287.

Other definitions are not quite as deferential. Another brand of hackers are referred to as "cyberpunks." Id. Cyberpunks are hackers who create harmful programs, such as viruses. Id. For the purposes of this Comment, a "hacker" is analogous to a cyberpunk—one who creates destructive programs for the sole purpose of causing damage to other systems.

29. Vandalism is defined as "[s]uch willful or malicious acts as are intended to damage or destroy property." BLACK'S LAW DICTIONARY 1553 (6th ed. 1990).

30. See Stang, supra note 21, (discussing amount of PCs in the United States).

31. On Friday March 6, 1992, the 517th birthday of Michaelangelo, at midnight, the world was struck with a new virus, named after the artist it was designed to celebrate. An estimated 5 million IBM and IBM-compatible computers were affected with this deadly virus that destroys huge amounts of data on the computers it enters. Barnet D. Wolf, Companies Vow to Fight Vicious Virus, COLUMBUS DISPATCH, Feb. 21, 1992, at 1C. "Michaelangelo," first detected in Sweden in 1991, infected computers all over the world,
which enjoyed significant media hype.

1. **Computer Viruses**

Although some would consider them to be a relatively new phenomenon, computer viruses have existed since at least the early 1960's. Today, the term has become a veritable household word, due as much to the colorful guises viruses assume, as to the widespread destruction that they cause. The creative and sometimes even humorous forms viruses take, however, must not detract from the gravity of

including the United States, Bolivia, and Uruguay. South Africa was reportedly the hardest hit however, with 1000 computers from nearly 500 companies—mostly pharmacies, wiped out. Joel Simon, *Software Firm Fights War Against Hackers*, DETROIT FREE PRESS, Mar. 6, 1992, at 3A. Fortunately, early detection of the virus caused a heightened awareness of Michaelangelo’s arrival, and computer users all over the globe worked together to make virus protection programs and other remedies available to users before the virus hit. *Id.* Unfortunately, not all users escaped in time and countless damage ensued.

32. One week after “Michaelangelo” left its trail of destruction, another virus struck on what was intended to be a regular occurrence. The “Jerusalem” virus was one hacker’s way of commemorating Israel’s declaration of statehood on May 14, 1948, by programming the virus to activate on May 13, 1988, and every subsequent Friday the 13th. *See* Stang, supra note 21. “Jerusalem” was first detected in July, 1987, and its mission was to insert itself into program files with either .EXE or .COM extensions, and erase them if they were run on Friday the 13th. *Id.* “Jerusalem,” also called “Friday the 13th,” is the second most common virus among PC users in the United States. Kerry Fehr, *PC Poison Michaelangelo Poised for March 6 Computer Assault*, PHOENIX GAZETTE, Feb. 26, 1992. Number one among viruses in the U.S. is the “Stoned” virus, which informs the user that his or her system is stoned, and then calls for the legalization of marijuana. *Id.* “Stoned” and “Jerusalem” account for nearly 85 percent of all virus infections among the top 1 percent of U.S. organizations using PCs. *Id.*

33. Computer viruses were popular among Ivy League college hackers in the 1960’s, primarily as a form of practical joking. R. Roberts, *Computer Viruses* 6 (1988). The idea was to insert a small code into a friend’s program to prevent it from running as he had intended. *Id.* at 9. Although these codes were not true viruses, they demonstrated the ability to disrupt another’s program, and consequently gave rise to their modern, more destructive successors. *Id.* at 10.

34. Viruses are generally characterized by their means of infecting their victims, such as the Trojan Horse-type virus. *See* Kluth, supra note 7, at 298. A Trojan Horse virus is a malicious program hidden within an ostensibly useful or recreational program such as a game. *Id.* By the time the user discovers the hidden virus, it is usually too late. *Id.* Other forms of viruses are “worms,” *see* supra note 7, and “bombs.” “Bombs” may be “logic bombs,” which are viruses with a delayed infection mechanism that allows them to infect back-up data before activating. Raymond Hansen, Note, *The Computer Virus Eradication Act of 1989: The War Against Computer Crime Continues*, 3 SOFTWARE L.J. 717, 733 n.70 (1990). A bomb may also be a “time bomb,” which means that the virus does not activate until a certain event occurs, such as a program being run a certain amount of times, or more commonly, upon a certain date. *Id.* Both “Michaelangelo” and “Jerusalem,” (see supra notes 31 and 32 respectively) are examples of “time bombs.”

35. The “Cookie Monster” virus would disrupt whatever program was running, and
their destructive purpose—essentially a form of high-tech terrorism.\textsuperscript{36}

The damages caused by computer viruses may take many forms,\textsuperscript{37} each having devastating potential.\textsuperscript{38} While some viruses destroy valuable data,\textsuperscript{39} others damage the computer system itself.\textsuperscript{40} Additionally, peripheral damages resulting from the virus may be considerable, as was the case with Robert Morris. The virus that Morris released into the INTERNET network destroyed no data, but caused considerable labor expenditures in removing the worm from the system.\textsuperscript{41} Another distressing aspect of computer viruses is the case of the computer voyeur,\textsuperscript{42} whose virus allows him access to others' files, but which causes no pecuniary or data damages at all. Essentially, computer virus display the message "I want a cookie!" See Branscomb, supra note 3, at 16 n.75. The user was unable to resume working on his or her program until discovering that the message would go away when "COOKIE" was entered on the keyboard. Id. On the more destructive side, one college virus program was listed as RCK.VIDEO. See Elmer-DeWitt, supra note 8. An animation featuring the rock star Madonna performing would appear on the screen when a user downloaded it. Id. When Madonna finished her act, she then announced to the viewer, "You're stupid to download to a video about rock stars." Id. The confused user would then discover that all files on the system had been erased. Id.

36. Some assert that small-scale viruses are similar to vandalism, while larger viruses are more akin to terrorism. See Kluth, supra note 7, at 297. One example of this high-tech terrorism is the German Chaos Computer Club, which operates out of Germany, and uses viruses and other computer resources to inflict damage on government computers all over the world. See Rosenthal, supra note 26. One of the systems which the Club managed to infiltrate was NASA's Space Physics Analysis Network. Id. Consequently, the potential for damage may extend to threatening national security.

37. See supra note 27 for a general discussion of the different effects of viruses. Also, see infra notes 45-49 for further examples of various damages caused by computer viruses.

38. See supra note 17 and accompanying text for an illustration of how monetary damages alone may be staggering, without even including lost time and other associated damages.


40. See infra note 108 for an illustration of how a virus can damage the computer itself, in addition to the data stored therein.

41. See supra note 17 for a discussion of the INTERNET worm damages.

42. A computer "voyeur" is one who accesses a network or system without authority, merely to see what is there. See Branscomb, supra note 3, at 36. The Computer Fraud and Abuse Act does not address this problem in the offenses that it proscribes. Id. The only possible section under which a voyeur could be prosecuted would be the misdemeanor offense of accessing without authorization a computer intended for exclusive governmental use. 18 U.S.C. § 1030(a)(3) (1986). Missouri responded to the problem of the computer voyeur by including in its computer crime statute the offense of using a computer for the purpose of intentionally examining another's information. MO. ANN. STAT. § 569.095(5) (Vernon Supp. 1989). Other states are more lenient towards the computer voyeur, and do not criminalize such activity. KY. REV. STAT. ANN. § 434.845 (Baldwin 1985). Kentucky specifically excludes voyeurism from criminal prosecution so long as that person's intention is only to "obtain information" and not to commit any other computer offenses. Id.
damage may be both amorphous\textsuperscript{43} and varied, according to the intent of the particular virus creator.

The propagator\textsuperscript{44} of a computer virus is motivated by several impulses, such as revenge,\textsuperscript{45} punishment,\textsuperscript{46} pranking,\textsuperscript{47} malice,\textsuperscript{48} or bra-

\begin{itemize}
\item \textsuperscript{43} An illustration of the amorphousness of these effects would be a virus that caused all D.U.I. convictions which occurred on July 4, 1992, to be deleted from a State's Department of Motor Vehicle computer system. Michael Gemignani, \textit{What is Computer Crime, and Why Should We Care?}, 10 U. ARK. LITTLE ROCK L.J. 55 n.5 (1988).
\item \textsuperscript{44} The creator of a computer virus is typically a European Anglo male between 17 and 28 years old. \textit{See} Williams, \textit{supra} note 27. He is most likely an underachiever who is trying to either get attention or to prove something by his actions. \textit{Id.} He may be a “social misfit” who finds computers easier to relate to than people; or perhaps a “brilliant teenager” who is trying to leave a form of computer graffiti; or he may even be a political activist trying to bring the system to its knees. \textit{See} Simon, \textit{supra} note 31.
\item \textsuperscript{45} In \textit{Burleson v. State}, 802 S.W.2d 429 (Tex. Ct. App. 1991), the defendant, the technical security officer for a brokerage house and insurance company, was fired for misusing the company's computers. \textit{Id.} at 433. Burleson had access to all of these computers and their passwords, and used them to enter the system and insert “time bombs” which deleted 168,000 of the company's sales commission records. \textit{Id.} Fortunately, the records had been backed-up, although it took a team of programmers an entire weekend to restore the system, which had to be shut down for four hours. \textit{Id.} at 434. Burleson was found guilty and given seven years of probation and assessed $11,800 in restitution. \textit{Id.} at 432.
\item \textsuperscript{46} Two Pakistani brothers in 1988 created the "Pakistani Brain" virus, which destroyed huge amounts of data, but was difficult to detect because it only infected MS-DOS formatted disks rather than the hard drive. \textit{See} Branscomb, \textit{supra} note 3, at 13 n.57. The brothers' intent was to punish local hackers who pirated their software. \textit{Id.} A message would appear telling the user “Because you are pirating, . . . [y]ou must be punished.” \textit{Id.} The user would then see the brothers' address and number which he or she would have to contact for decontamination instructions. \textit{Id.} The virus spread all over the world, and one infection alone at George Washington University affected an estimated 10,000 users. \textit{Id.}
\item \textsuperscript{47} Some pranksters feel a need to gloat after destroying someone's data. One such virus devoured all of the memory from a computer, as well as any work currently in progress, and upon completion of the destruction, informed the user, “Arf, arf, Gotcha!” \textit{See} Elmer-DeWitt, \textit{supra} note 8.
\item \textsuperscript{48} Kevin David Mitnick was a 25-year old hacker with a history of legal troubles stemming from countless invasions into computer networks. Kim Murphy, \textit{Computer Whiz Admits Criminal Mischief}, \textit{L.A. TIMES}, Mar. 16, 1989, at 3. He fancied himself as a crafty computer rogue, assuming the name “Condor,” and constantly used his computer knowledge to outwit the government. \textit{Id.} His actions were malicious and compulsive, and a friend claimed that not a day went by without Mitnick infiltrating some unauthorized network. John Johnson, \textit{Computer and “Umbilical Cord to his Soul,” } \textit{L.A. TIMES}, Jan. 8, 1989, at 29. One judge who had sentenced Mitnick to a reformatory, found his credit
\end{itemize}
vado.49 Whatever the motive or whatever legitimacy the virus creator ascribes to his actions, such a person is merely a criminal. Stripped of the colorful names, assumed identities, and complex designs, these hackers amount to little more than common vandals with a keyboard. Rather than remark how clever hackers seem, we must recognize the underlying malice or recklessness, and move to eliminate such conduct. This was Congress' intent in enacting the Computer Fraud and Abuse Act of 1986.50

2. The Computer Fraud and Abuse Act

In 1986, the United States Congress passed the Computer Fraud and Abuse Act, as a response to the growing problem of computer crime.51 The Act provides for three separate felonies and three misdemeanors. Initially, the Act makes it a felony to knowingly52 access a computer without authorization and to obtain national defense information with the intent to use such information to harm the United States.53 The Act also makes it a felony to access a federal interest computer,54 with the intent to defraud, and to obtain anything of

49. 18 year old Herbert Zinn assumed the identity of “Shadow Hawk,” when he broke into government computers. W. Alexander, Prison Term for First U.S. Hacker-Law Convict, COMPUTERWORLD, Feb. 20, 1989, at 1. Zinn infiltrated AT&T’s Bell Laboratory computers, as well as NAO and U.S. Air Force facilities, merely because he could, and stole highly-sensitive source codes, according to the Department of Justice. Id. Zinn was eventually arrested and convicted for this break-in and sentenced to nine months in jail and assessed a $10,000 fine which the judge ordered that he, not his parents, pay. Id.


51. Id.

52. The mens rea requirement of “knowingly” is satisfied when the defendant intentionally performs some act with the knowledge that, in the particular circumstances, the results the defendant intends are practically certain to occur. MODEL PENAL CODE § 2.02 General Requirements on Culpability (Official Draft 1985).

53. 18 U.S.C. § 1030(a)(1) (1992). More specifically, the Act proscribes knowingly accessing or exceeding authorized access to obtain national defense, foreign relations, or other such classified information with the knowledge or belief that doing so will harm the United States, or benefit another country. Christopher Chen, Note, Computer Crime and the Computer Fraud and Abuse Act of 1986, 10 COMPUTER L.J. 71, 77 (1990).

54. The Act defines a “federal interest computer” as a computer:

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

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State. . . .
value. The third and final felony in the Act is altering or damaging information in a federal interest computer, causing losses exceeding $1000, or interfering with one or more person's medical care. A violation of any one of these three sections subjects a first-time offender to a possible fine, up to a ten-year sentence, or both.

It is a misdemeanor under the Act to access a computer without authorization, in order to obtain information from a financial institution. The second misdemeanor is accessing, without authorization, any computer designated for exclusive government use. The third misdemeanor offense is trafficking passwords or other related access information such that interstate commerce is affected. All misdemeanors are punishable by up to one-year imprisonment, a fine, or both.

Only one section of the Act addresses the actual amount of damages which are caused in the course of violating it. This is significant because computer viruses have an awesome potential to cause great amounts of damage and permanent loss. Additionally, that section which does address damages pertains only to interference with federal interest computers. The Act criminalizes damaging a federal interest computer in excess of $1000, but that amount is merely an element of the crime, rather than a gauge for sentencing. Clearly there is a major deficiency in the Act when the sentencing portion does not account for the amount of damages in fixing an appropriate penalty. Nowhere is this flaw more compelling than in the case of Robert Tappan Morris.

---

55. Id. § 1030(a)(4). Note that merely using the computer does not suffice to violate this section, but rather something of value must be taken. Id.
56. Id. § 1030(a)(5).
57. 18 U.S.C. § 1030(c) (1992). The penalties for subsequent offenses are obviously more severe. After the original offense, repeat offenders face up to twenty years in prison. Id.
58. Id. § 1030(a)(2).
59. Id. § 1030(a)(3). Additionally, if a computer is intended for only partial government use, this section will be violated if the defendant in any way interfered with the government's access. Id.
60. Id. § 1030(a)(6).
61. Id. § 1030(c)(2)(A). Recidivism is punishable by a ten-year sentence under this section. Id.
62. Id. § 1030(a)(5) (punishing those who commit in excess of $1000 damage).
63. See supra note 17 for a discussion of the immense damages caused by computer viruses.
64. Id. § 1030(a)(5).
65. Id. § 1030(a)(5).
66. See supra note 1.
III. A NEW METHOD OF COMPUTER VIRUS SENTENCING-SETTING PUNISHMENTS ACCORDING TO THE DAMAGE CAUSED

While the Computer Fraud and Abuse Act of 1986\textsuperscript{67} effectively proscribes spreading computer viruses, the Act fails to provide appropriate penalties for those convicted under it. The \textit{Morris} case\textsuperscript{68} clearly demonstrates this inadequacy. Robert Tappan Morris intentionally created a virus and then inserted it into a national computer network.\textsuperscript{69} His intentions to create damage were clear and unequivocal,\textsuperscript{70} despite his own claims to the contrary.\textsuperscript{71} The virus then went on to cause millions of dollars in damages.\textsuperscript{72} Despite all of the financial damage he caused, all of the grief he caused, and all of the irreparable harm to the people whose work and research were affected, Morris' punishment was a suspended sentence, community service, and a grossly inadequate fine.\textsuperscript{73} The court should have sent a strong message not only to the defendant, but more importantly, to other potential virus propagators, that such behavior would be dealt with swiftly and severely. Instead, what the court gave Morris amounted to a slap on the wrist.\textsuperscript{74}

The inadequate sentence should not be blamed on the sentencing court, but rather on the Act itself. The sentencing portion of the Act\textsuperscript{75} needs to be restructured in order to give better guidance to the courts. A major problem with prosecuting the people who create computer viruses is that the effects of these programs differ vastly from one virus to the next.\textsuperscript{76} Consequently, one virus may cause little or no damage.

\textsuperscript{68} United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
\textsuperscript{69} See supra note 11 (discussing Morris' method of creating the INTERNET worm).
\textsuperscript{70} The Commission authorized to investigate the INTERNET worm concluded that Morris had not intended for the worm to damage or destroy any data. The Commission further concluded however, that given the consequences of the virus' replication, and the intricacy of the design of the worm which he created, Morris' actions were either malicious, or done without regard to the potential damage. T. Eisenberg et al., \textit{The Computer Worm: A Report to the Provost of Cornell University on an Investigation Conducted by the Commission of Preliminary Enquiry}, 9-10 (Feb. 6, 1989). The commission found it difficult to reconcile the degree of intelligence demonstrated by Morris with the consequences of the virus, and speculated that Morris "did not pause to consider the potential consequences of his actions," and further that he was so "focussed [sic] on the minutiae of tactical issues that he failed to contemplate the overall potential impact of his creation." Id. at 30-31.
\textsuperscript{71} See supra note 14 (discussing Morris' claim that the vast amount of damage was not planned, but rather the product of a programming error).
\textsuperscript{72} See supra note 17 (discussing damages caused by the INTERNET worm).
\textsuperscript{73} See supra note 18 (discussing Morris' sentence).
\textsuperscript{74} Id.
\textsuperscript{75} 18 U.S.C. § 1030(c).
\textsuperscript{76} Contrast the damages caused by the "Jerusalem" virus, (see supra note 32), which
while another could disable an entire network. The Act needs to be re-
efined so that sentencing is tailored to the individual and the particular
virus created by that individual. This would be accomplished by incor-
porating into the Act a scale that would set punishments according to a
certain factor that would vary from case to case. The factor used to de-
terminate the severity of the sentence would simply be the amount of
damage done.

A. THE AGGRAVATED SENTENCING SCALE

The aggravated sliding scale is an effective and proven way of let-
ting the punishment fit the crime. Such a system works to either de-
fine an offense or calculate the sentence for that crime. The scale
operates with one element, not necessarily an element of the crime, se-

has destroyed immeasurable data and has paralyzed computers worldwide, with the mere
inconvenience of a virus such as “Cascade,” which causes the letters on the monitor to
drop to the bottom of the screen. Harry Rosenthal, Virus Busters Computer Software
Screens the Villains, ARIZONA REPUBLIC, Wed. July 17, 1991 at 7S17. Obviously, there is a
need to ensure that the punishment given to the offender who creates the destructive
equivalent of “Jerusalem,” does not approximate the punishment handed down to the
programmer of a “Cascade”-type virus. Id.

77. Perhaps the leading case to affirm the constitutionality of an aggravated sentenc-
ing scheme is McMillan v. Pennsylvania, 477 U.S. 79 (1986). In McMillan, the Court con-
sidered a Pennsylvania statute which mandated a minimum five-year sentence when the
defendant has been found by a preponderance of the evidence to have “visibly possessed a
firearm” during the commission of certain felonies. 477 U.S. at 81. The essence of the
defendant’s argument was that an aggravating factor, in this case, the visible possession
of a firearm, should be treated as an element of the offense, and thus need be established
beyond a reasonable doubt. Id. at 82. The Court disagreed, holding that whenever an off-
fense links the “severity of the punishment” with the “presence or absence of an identi-

fied fact,” that fact need not be proved beyond a reasonable doubt, but rather by a
preponderance of the evidence. Critically, the Court noted that an aggravated sentencing
scheme did not affect the burden of proof of either side, but only served to limit the sen-
tencing court’s discretion in choosing an appropriate penalty. Id. at 87. The import of this
decision is that the sentencing court may consider factors extrinsic from the mere ele-
ments of an offense to set the punishment. The validity of the scheme is founded in the
premise that aggravated sentencing determinations are not considered until the prosecu-
ction has proved all elements of the offense beyond a reasonable doubt. In McMillan,
therefore, the fact that the defendant displayed a gun during the commission of his off-
fense, in no way swayed the court’s determination of guilt at the trial stage.

78. The crime of aggravated rape is a distinct and more severe offense than simple
rape, in that all rape elements are present, plus other aggravating factors. One example
of the addition of aggravating factors to elevate the severity of an offense is the Massachu-
setts Aggravated Rape statute. MASS. GEN. LAWS ANN. ch. 265 § 22(a) (West 1992). The
crime of rape is generally sexual intercourse by a person with another person who is com-
pelled to submit by force and against his or her will, or through some threat of force. Id.
If certain other elements are present in the commission of the offense, however, the crime
is elevated to aggravated rape. Id. Factors designated to aggravate the crime of rape are:
committing bodily injury, committing the rape in a joint enterprise, or committing the
rape during the commission of some other felony. Id. ch. 277 § 39 (West 1992). The pres-
lected as the aggravating factor.\textsuperscript{79} The severity of the punishment then depends on the presence or absence of that factor.\textsuperscript{80} In the case of computer viruses, the scale would serve to let the punishment fit the damage. The aggravating factor would be the damage caused by the virus. A relatively harmless virus would receive a commensurate slap on the wrist, while more harmful viruses could lead to significant fines or jail time.

Initially, one must note the importance of the fact that the courts will only consider the amount of damages caused by the defendant after that person has been convicted.\textsuperscript{81} Therefore, a presumption of guilt will not arise from the amount of damage caused.\textsuperscript{82} Accordingly, the fact finder will not be biased in favor of either the defendant or the prosecution.\textsuperscript{83} A contrary result would result in Due Process violations.\textsuperscript{84} Only when the prosecution has established the defendant’s guilt would the

\begin{flushright}
\begin{footnotesize}
\textsuperscript{79}. Just as certain elements may be taken into consideration for the purposes of increasing a sentence, the converse may also be true. Factors may also serve to reduce the austerity of a penalty. Factors sometimes used to mitigate a sentence are: a lack of prior criminal history, the fact that the victim of the crime may have participated in the defendant’s conduct, the defendant acted under duress or under another person’s dominion, or the defendant at the time of the offense could not appreciate the criminality of his conduct. \textit{Mass. Gen. Laws Ann. ch. 279 § 69(b)} (West 1992). Thus a sentencing scheme based on aggravating factors is not designed for the sole purpose of increasing a defendant’s sentence, but rather to add a degree of subjectivity which will allow for a more appropriate penalty.

\textsuperscript{80}. \textit{Patterson v. New York}, 432 U.S. 197 (1977). (state need not “prove beyond a reasonable doubt every fact, the existence or nonexistence of which it is willing to recognize as an exculpatory or mitigating circumstance affecting the degree of culpability or the severity of the punishment”).

\textsuperscript{81}. Section 1030(a)(5)(A) of the Act which requires $1000 damage be committed, would still remain as an element of the offense, as separate from the aggregate amount of damage caused, which would apply only to sentencing determinations.

\textsuperscript{82}. \textit{Adamson v. Ricketts}, 865 F.2d 1011, 1054 (9th Cir. 1988). The court noted that the constitutional validity of an aggravated sentencing scale was supported by the notion that the aggravating factor did not alter the presumption of innocence and that the prosecution must still prove all elements of the crime beyond a reasonable doubt. \textit{Id}.

\textsuperscript{83}. “From the vantage point of the Constitution, a change in law favorable to defendants is not necessarily good, nor is an innovation favorable to the prosecution necessarily bad.” John C. Jeffries, Jr. & Paul B. Stephan III, \textit{Defenses, Presumptions, and the Burden of Proof in the Criminal Law}, 88 \textit{Yale L.J.} 1325, 1361 (1979).

\textsuperscript{84}. Due process limits insure that the burdens of proof in criminal cases are not reallocated or reduced in favor of either side. \textit{McMillan v. Pennsylvania}, 477 U.S. 79, 86 (1986). Although the \textit{McMillan} Court affirmed that a sentencing factor need not be an element of the offense, it cautioned that state legislatures are still bound to act within the boundaries of due process. \textit{Id.} at 87. Specifically, “[i]t is not within the province of a legislature to declare an individual guilty or presumptively guilty of a crime.” \textit{Id.}; cf. \textit{McFarland v. American Sugar Refg. Co.}, 241 U.S. 79, 86 (1916).
\end{footnotesize}
\end{flushright}
scale activate. The most appealing aspect of such a sliding scale is that the punishment not only fits the crime, but more significantly, it fits the consequences. This is especially satisfying in a society like ours, which punishes results. Several aspects of our laws support this assertion. In criminal law, results are factors in determining the punishment under the felony-murder doctrine, as well as in drug prosecutions. In civil law, the eggshell skull rule serves to punish according to the final outcome.

1. Drug Offense Prosecution

The criminal system is one such area of law that punishes results. One area of law where results are factored into punishment is in the prosecution of drug offenses. Defendants convicted of possessing controlled substances are punished according to the quantity of the controlled substance involved. The greater the amount found in the possession of the defendant, the longer the minimum sentence becomes. Such a sentencing scheme has withstood numerous constitutional challenges, and has consistently been affirmed by the nation's laws.

85. The burden still rests on the prosecution to prove beyond a reasonable doubt that all elements of the crime have been established. McMillan, 477 U.S. at 87. This format preserves the policy behind the Act—that the prosecutions must focus on those who evince a clear intent to cause damage through unauthorized access, rather than encompassing those whose unauthorized access was purely unintentional. S. Rep. No. 99-432, 99th Cong., 2d Sess. 5 (1986).


87. Id.

88. See United States v. Mendes, 912 F.2d 434, 439 (10th Cir. 1990) (statute providing for minimum sentence for those dealing in large amounts of drugs did not violate defendant's equal protection or due process rights); United States v. Murphy, 899 F.2d 714, 717 (8th Cir. 1990) (Federal Sentencing Guideline which required defendant's offense level to be calculated based on entire weight of methamphetamine mixture involved, without regard to mixture's purity, did not violate defendant's due process rights); United States v. Bishop, 894 F.2d 981, 986-87 (8th Cir. 1990) (combined weight was properly considered for sentencing purposes, and basing sentences on quantity without regard to purity did not violate due process); United States v. Holmes, 838 F.2d 1175, 1177-78 (11th Cir.), cert. denied, 486 U.S. 1058 (1988) (within congressionally established range for sentences, nothing in statute restricts discretion of sentencing judge in fashioning individualized sentence in light of specific facts of offense and history of offender); United States v. Klein, 860 F.2d 1489, 1501 (9th Cir. 1988) (imposition of mandatory minimum sentence upon conviction of possession with intent to distribute did not violate defendant's due process or equal protection rights, in that basing of minimum sentence on quantity rather than quality of substance was reasonably related to congressional intent to deal more severely with large volume narcotics dealers); United States v. Hoyt, 879 F.2d 505, 512 (9th Cir. 1988) (court affirmed validity of statute which set classifications by punishing person who sells small
highest court. Once the Government proves the defendant's guilt beyond a reasonable doubt, the defendant becomes liable for whatever penalty has been statutorily authorized for his offense.

Significantly, courts have found sentencing based on aggravating factors to be an effective means of carrying out congressional intent. Congress has expressed its clear and unequivocal intention to curb drug trafficking by attacking the upper-echelons of the industry where the drugs are manufactured and distributed. Consequently, Congress chose as its method of enforcing its intent, an aggravated sliding scale, with the aggravating factor being the amount of drugs involved. Imposing more severe penalties on those convicted of possessing or distributing larger quantities provides a rational basis for punishing offenders because it introduces consistency into sentencing by providing prescribed severe sentences for equally serious offenses.

2. Felony-Murder Prosecution

Another area of law where such an aggravated sentencing scheme has been utilized is in felony-murder prosecutions. Under the felony-murder doctrine, all persons aiding and abetting the commission of a felony are guilty of the crime of murder, when one of them kills a person while acting in furtherance of their crime. Therefore, the defendant...
ant is held vicariously responsible for the acts of his co-conspirators.97

The California State Supreme Court engaged in one of the most comprehensive discussions of the felony-murder doctrine in People v. Washington.98 In Washington, the defendant and his accomplice attempted to rob a gas station, but were single-handedly thwarted by the proprietor who shot and killed one man and wounded the defendant.99 Although only one defendant committed the fatal shooting, because a death resulted, both defendants were charged with murder, just as if both had pulled the trigger. Discussing the felony-murder doctrine, Chief Justice Traynor noted that one of the main principles behind this doctrine is deterrence.100 Because all of the defendants are held vicariously liable when one commits a murder, it is believed that the number of murders will be reduced.101 Thus the court punishes the defendant based on the end result of the crime—the murder, and not necessarily based on the particular crime the defendant was committing.

Likewise, a sliding scale that governs sentencing for computer virus crimes would punish a defendant according to the ultimate results of the virus that he spread—the damages caused. Once the prosecution establishes that a defendant violated the Act, the court could then examine the damages and set the sentence according to the severity of the damages. Such a result would relieve the judges of much of his or her discretion, which seems appropriate for such a nascent area of law.102

3. The Eggshell Skull Doctrine

In civil lawsuits, the "eggshell skull" doctrine provides for liability for the full consequences of tortious actions, even if the plaintiff had preexisting conditions that made him or her more vulnerable to injury.103 The essence of this rule is that if the defendant caused the in-

---

97. Id.
98. Id.
99. Id.
100. Specifically, the court stated that the purpose behind the felony-murder rule is "to deter felons from killing negligently or accidentally by holding them strictly responsible for killings they commit." Id. at 133.
102. Ex Parte United States, 242 U.S. 27, 42 (1916) (defendant sentenced to the minimum 5 year sentence for embezzling and court exercised its discretion to temporarily stay the sentence "during the good behavior" of the defendant; court held relieving the judiciary of sentencing discretion was a valid exercise).
103. The leading case dealing with the "eggshell skull" doctrine was heard over 100 years ago, in 1891, when one boy kicked another, causing severe injuries. Vosburg v. Putney, 50 N.W. 403 (Wis. 1891). Since Vosburg, the doctrine has remained intact, and still endures in modern tort law. Niehus v. Liberio, 1992 WL 201110 (7th Cir. (Ill.)). Most recently, the United States Court of Appeals for the Seventh Circuit heard a case dealing with this doctrine and affirmed a jury award for the plaintiff. Id. In Niehus, after being
jury, he or she is liable, even though the plaintiff's physical condition might have aggravated the injury.\textsuperscript{104} This rule does not punish the defendant's act, nor does it look at the person's state of mind when he or she acted tortiously. Rather, the rule considers only the consequences of that defendant's act, and allows the result to determine the punishment.\textsuperscript{105}

Thus, the eggshell skull rule, drug offense prosecution, and the felony-murder doctrine each demonstrate that a sentencing scale based on results as an aggravating factor is an effective and just way of punishing crimes. This system permits courts to look beyond the mere elements of the crime and at the end result, in order to fix an appropriate penalty. Having established the fairness and utility of such a system, the next task is determining how to measure the aggravating factor, so as to establish the range of the sentencing scale.

\section*{B. QUANTIFYING THE DAMAGE DONE}

The threshold dilemma then becomes determining the easiest and most effective method of quantifying the particular damage that is left in the wake of a computer virus. However, the potential amorphousness of virus damage should in no way deter prosecutors and courts from fixing appropriate sentences for convicted offenders. Several avenues are available by which values can be placed on virus damage, such as financial losses, lost data, and lost operation time.

1. \textit{Monetary Losses}

The damage a computer virus causes can be quantified fairly easily through the monetary losses suffered by users. Users who are infected by a virus often are faced with a variety of costs in repair, replacement involved in an accident the plaintiff was arrested for drunk driving. In the course of a struggle, the defendant police officers kicked him in the face. \textit{Id.} The plaintiff suffered a broken cheekbone. \textit{Id.} In addition to the cheekbone injury, the plaintiff suffered permanent brain damage resulting in partially disabling mental and emotional injury. \textit{Id.} The court affirmed the jury verdict in favor of the plaintiff, holding that because the defendant had kicked the plaintiff in the face, the fact that the cheekbone may have already been broken would not exculpate the defendants in any way. \textit{Id.} Consequently, the defendants were held liable for the "full consequences of their kicks even if, had it not been for a preexisting injury, the consequences would have been much less injurious." \textit{Id.} at 2.


105. A far-fetched example is the defendant who, out of pure spite, sticks somebody on the arm with a thumbtack. Unbeknownst to that defendant however, the victim suffers from hemophilia, and subsequently bleeds to death. The defendant would be held accountable for the victim's death, just as if he had stabbed him in the heart.
of equipment, and labor costs. Monetary damages are concrete and thus are especially useful in creating a scale for sentencing. The scale would begin at a certain dollar amount and continue perhaps ad infinitum, with corresponding penalties at various dollar amounts. The aggregate monetary damage would be the determining factor on the scale.

Some viruses may destroy not only data, but also damage the computer itself, in which case the replacement cost of lost equipment would be the proper gauge. Repair costs are also an effective method of monitoring the effects of a virus. When a system becomes infected, experts must come in and remove the virus from the system, usually at considerable expense to the user. Re-entering lost data into a system also requires long hours, providing of course, that the information has not been permanently destroyed. Labor costs would certainly be factored into a victim's losses. Additionally, the court would not be required to pinpoint the exact amount of pecuniary damage caused by the virus, but rather make a reasonable estimate. The court could base

106. See supra note 109 for a discussion of the labor costs involved with removing a computer virus from an infected system.


108. The “Alameda” virus not only destroys data, but also damages the boot sector of a computer by overriding the original boot sector instructions. See Hansen, supra note 34, at note 26. The effect of this virus is that it replaces the boot sector codes with its own instructions, and thus the boot sector allows the virus to move throughout the system, infecting files, and eventually crashing the entire system. Id.

109. The costs of disinfecting a computer system could be staggering. A conservative estimate of computer infection in the United States alone is one percent. See Stang, supra note 21. This amounts to approximately 500,000 computers. Id. Further, assuming that it would take a mere 20 hours to disinfect a system, at a conservative estimate of a $15 per hour service charge, the national bill for only a one percent infection rate would be $150 million. Id. A survey conducted in 1989 however, found that 10 percent of the respondents had personally suffered a computer virus, and that 23 percent knew of someone who had been infected. Id. This suggests a far greater amount of monetary damages. In the private sector, one corporation in Texas was infected, requiring its 3,000 computer network to shut down for four days. Id. It took 50 computer analysts to remove the virus, even though the team discovered that only 35 computers were actually infected. Id. The total costs to the corporation however, including lost revenues, was $10 million. Id. Unfortunately, even having a virus removed provides no guarantee of safety from further virus harm. Id. In the United States, 90 percent of all infected users experience re-infection within 30 days of having the original virus removed. Id.

110. Id.

111. Using monetary losses as the aggravating factor for the sentencing scale would be effective in that the court would not be required to pinpoint an exact amount of damage inflicted by the virus, but rather it would only need to make a reasonable estimate. Fed. Sent. Law & Prac. § 2FL1.1, note 8 (West 1992). “The amount of loss need not be precise. The court is not expected to identify each victim and the loss suffered to arrive at an exact figure.” Id.
its estimate on the monetary damages caused by other viruses, and look to these other viruses as a proper guide for sentencing. Consequently, there are several ways by which financial losses can be computed, which makes a pecuniary sentencing scheme particularly desirable.

Conversely, the one problem with a monetary scale is its dependence on users reporting their losses.\textsuperscript{112} Assuming that people are willing to take the time to report losses stemming from computer viruses, it is unclear to some as to whom a computer virus should be reported.\textsuperscript{113} Additionally, another reporting problem is encouraging victims to actually come forward and report the crimes.\textsuperscript{114} The negative publicity associated with virus infection keeps many businesses from reporting such infections, for fear that some will view an infection as a weakness.\textsuperscript{115}

While this may not be the most definitive means of calculating total losses, it is certainly a viable and effective option. Additionally, for the scale to work, the prosecution need not prove all losses beyond a reasonable doubt, but merely by a preponderance of the evidence.\textsuperscript{116} Given the success in estimating damages of prior viruses, the numerous methods of computing financial loss, and the availability of efficient reporting services for affected users, a pecuniary loss scale would be the most successful agent to use as an aggravating factor.

2. \textit{Lost Data}

A more obtuse facet of computer virus damage is the data or infor-

\begin{footnotesize}
\begin{enumerate}
\item[\textsuperscript{112}] Some suggest that strict liability be imposed on employers to report virus infections, and known perpetrators. \textit{See} Branscomb, \textit{supra} note 3, at 55. Certain states have imposed such duties on infected users. \textit{Ga. Code Ann.} § 16-9-95 (1988); \textit{Utah Code Ann.} § 76-6-705 (1989). The major problem with imposing a duty to report on infected users is that while a private individual may be willing to report infection, more often than not, larger businesses and corporations will not. Telephone interview with Raymond Glath, President of RG Software Systems, Inc., Scottsdale, AZ (October 16, 1992). Computer virus infection carries with it an \textit{"achilles-heel"} stigma in the business community. \textit{Id.} A business that has been infected often will opt to assume the financial losses and not report the infection because other businesses tend to view infection as a weakness. \textit{Id.}

\item[\textsuperscript{113}] One survey showed that out of 148 respondents who had suffered some form of computer crime, only 40 respondents reported the incidents to the authorities. \textit{See} Gemignani, \textit{supra} note 99, n.6. Of the respondents, 143 took some form of action against the perpetrator. \textit{Id.} In 54 cases, the perpetrator was identified and prosecuted, however only 15 defendants were sentenced or fined, while 21 other cases were still pending. \textit{Id.} Clearly there is a need for vigorous prosecution of computer virus crimes in order to encourage victims to report virus infections. \textit{Id.} A high success rate would serve as an incentive to victims to report computer viruses, when the victims know that their harm will not go unanswered.

\item[\textsuperscript{114}] \textit{See} Hansen, \textit{supra} note 34.

\item[\textsuperscript{115}] \textit{See} \textit{supra} note 113, interview with Raymond Glath.

\item[\textsuperscript{116}] \textit{See} \textit{supra} note 77 (discussing how the aggravating element need not be proven beyond a reasonable doubt, but merely by a preponderance of the evidence).
\end{enumerate}
\end{footnotesize}
information that is lost. While some information is replaceable due to backup records or disks, other information may be permanently lost due to a destructive virus.\textsuperscript{117} Consider the student who is fervently working on her paper into the early morning hours. Just as she is about to begin her eloquent conclusion, a virus hits her PC, and fifteen pages of text are lost forever. What value could be placed on her lost work and could her loss ever be verified? The major problem with attempting to use lost data as the basis for a sliding scale is that it is difficult to place a value on intangible property.\textsuperscript{118} A potential solution to this pervasive problem would be to simply count the number of people who permanently lost data. The number of affected people would then become the aggravating factor.\textsuperscript{119}

Although no one would dispute that lost data is a very real and potentially paralyzing effect of computer viruses, until a way to appraise the lost information is developed, it is not an appropriate factor by which a sentencing scale could operate.

3. Lost Operation Time

An exceedingly vexing effect of a computer virus is the computer time that is lost while the system is either infected, or being repaired. This is more concrete than simply lost data, and can be given a monetary value if necessary. Some state computer statutes have separate provisions for lost computer time,\textsuperscript{120} and use it as an element of the offense, rather than as an aggravating factor. Essentially, however,

\textsuperscript{117} The “nVir” virus is a particularly insidious data-consuming virus which infects Apple MacIntosh computers. \textit{See} Hansen, \textit{supra} note 34, n.27. It appears in several forms, and emits a “beep” sound as it begins its destructive mission. \textit{Id.} MacIntosh users with Mac Talk will hear a “don't panic” message, while files begin to disappear. \textit{Id.}

\textsuperscript{118} Some states have attempted to include computer-stored data in definitions of property. Montana includes in its definition of property, “electronic impulses, electronically processed or produced data or information . . . computer software or computer program,” as well as computer services. \textit{Mont. Code Ann.} \textsection 45-2-101(54)(k) (1987). Another perspective is found in the Massachusetts definition of property, which includes “electronically processed or stored data, either tangible or intangible,” as well as “data in transit . . .” \textit{Mass. Gen. Laws Ann.} ch. 266, \textsection 30(2) (West Supp. 1988). While these definitions may adequately address the need to include computer-stored data as “property,” the problem of placing a value on the information still persists.

\textsuperscript{119} Approximating the number of victims and estimating the average loss to each one is another appropriate gauge for sentencing. \textit{Fed. Sent. Law & Prac.} \textsection 2F1.1(8) (West 1992). Even more generally, the nature and duration of the offense might be considered in fixing a penalty for a convicted hacker. \textit{Id.}

\textsuperscript{120} An example of such a state statute is the Wyoming computer crime statute, which prohibits “denying services to an authorized user.” \textit{Wyo. Stat.} \textsection 6-3-504(a) (1988). Thus a person who creates a virus which either shuts the victim's computer system down, or prevents the user from accessing the system, renders himself criminally liable under this statute. \textit{Id.}
"down time" could be an effective gauge for certain viruses that prevent any authorized use of a network or system. By calculating the number of users at the time the virus struck, or even determining an average amount of authorized users on the system, and then multiplying the amount by the amount of time the system was down, concrete figures would result.

If necessary, a monetary value could be assigned to one hour of online time. If the virus spread through disks, rather than through a network, a system similar to what was proposed in the section dealing with pecuniary loss could be employed—a user-friendly and efficient reporting system that would be made available to affected users. This system would be most effective with "harmless," self-eradicating viruses which did not destroy data or equipment, but rather rendered systems inoperable for short periods of time.

Lost data and lost operation time are both valid approaches to gauging damages for the purpose of aggravating a sentence, but are by no means the only available options for doing so. Depending on the particular virus, other factors may be more appropriate. Although lost data and lost operation time are potentially workable aggravating factors for a sliding sentencing scale, clearly the most effective and easily-determined factor is the measure of pecuniary loss caused by the virus.

IV. CONCLUSION

The computer virus epidemic poses a serious danger to our society. Viruses have threatened national defense, destroyed tremendous amounts of data, and caused billions of dollars in monetary damages. The Computer Fraud and Abuse Act is a powerful weapon in combating this high-tech plague. However, the Morris case demonstrates that there is a clear need to amend the sentencing portion of the Act. This need would be eliminated by allocating sentences according to the damages caused by the convicted virus propagator. Similar aggravated sentencing scales have proven effective in both criminal and civil law, and would serve to deter future virus creators from spreading their malicious programs. The time for viewing computer viruses as a form of innocent pranking has long passed. It is time to see computer virus propagators for what they truly are—common criminals.

Joseph P. Daly

121. Other potential considerations for aggravating factors are: the objective behind the virus; any risks of physical harm posed by the virus (such as a virus which affected medical computers); the extent to which a virus might have threatened national security; or perhaps the damage done to an institution’s reputation which has been infected by the virus. FED. SENT. & PRAC. § 2F1.1(9).