3-1-1991

Computer Viruses and the Criminal Law: A Diagnosis and A Prescription

Paul Chastain Ray

Follow this and additional works at: http://readingroom.law.gsu.edu/gsulr

Part of the Law Commons

Recommended Citation
Available at: http://readingroom.law.gsu.edu/gsulr/vol7/iss2/6

This Article is brought to you for free and open access by the Publications at Reading Room. It has been accepted for inclusion in Georgia State University Law Review by an authorized editor of Reading Room. For more information, please contact jgermann@gsu.edu.
COMPUTER VIRUSES AND THE CRIMINAL LAW: A DIAGNOSIS AND A PRESCRIPTION

INTRODUCTION

Computer viruses impact society, both in the public perception and in the daily lives of average citizens. From January to July 1988, more than 300 viruses hindered the operation of over 50,000 computers.\(^1\) Many newspaper and magazine articles reported the famous computer virus of November 2, 1988, which was spread by Cornell University graduate student Robert T. Morris.\(^2\) Investigators estimate that the Cornell virus caused direct harm to some 6,000 computers on an extended network containing approximately 250,000 computers.\(^3\) Computer viruses also affect national defense,\(^4\) commercially-licensed software, and publicly-shared programs on electronic bulletin board services (BBS).\(^5\)

Federal law punishes several important areas of computer abuse, such as accessing national defense records, financial records, and medical records without authorization.\(^6\) The federal statutes do not explicitly address the spreading of computer viruses, however. No reported cases have applied a federal statute to the act of spreading a computer virus. In 1989, California, Illinois, Maine, Minnesota, and Texas became the first states to enact statutes that expressly address computer viruses.\(^7\) Other states' statutes prohibit a variety

---

4. Wilcox, supra note 2.
5. Bigelow, *Computer Security and Privacy*, 10 THE COMPUTER LAWYER 11-12 (Feb. 1989). Electronic bulletin board services promote the exchange of computer programs via telephone transmission between computer users. Commercial computer networks permit home computer users to access news wires, travel information, and messages and trial “shareware” programs from other users. Id.
of computer abuses, but as of January 1, 1991, no reported state court opinions had applied these state statutes in a case involving the spreading of computer viruses.

This Note describes the development of computer viruses, explaining what they are, how they originate, and how to fight them. The Note then summarizes the various ways in which the state computer crime statutes define substantive offenses and classify penalties, and identifies problems inherent in the various statutory approaches. A sample of state case law demonstrates the difficulty of defining computer abuse, interpreting imprecisely drafted legislation, and applying traditional criminal law to computer crimes.

This Note also questions the present ability of the federal computer crime statutes to fully address the computer virus problem. Federal case law illustrates judicial concern for the competing policies of protecting: (1) freedom of access to computer information, (2) property rights to computer data, and (3) regulatory jurisdiction over interstate commerce affected by computers. Because of these policy concerns, and because prosecutors lack the technological expertise required to fight the spreading computer virus problem, a need for legislative attention exists at both the federal and state levels. This Note proposes a federal statute to combat the computer crime epidemic and concludes that research and monitoring of computer viruses must continue.

I. DEVELOPMENT OF THE COMPUTER VIRUS PROBLEM

A. What Are Computer Viruses?

Computer viruses are small programs that copy themselves onto other programs or computer systems. Research has identified over thirty virus strains or types; hundreds of variations can exist,

15. McAfee, supra note 1, at 30.
however. The Department of Justice has identified a number of common computer crimes that computer viruses can facilitate.

Viruses are spread either internally or externally. Internal viruses must find programs with enough internal free memory to

16. Id.

17. S. LIPNER AND S. KALMAN, COMPUTER LAW CASES AND MATERIALS, 532—39 (1989) [hereinafter S. Lipner]. "Data leakage" is a method of obtaining unauthorized access to information by transferring data to areas where the perpetrator may collect it, disguising it as a report or less suspicious form of printout. Id. at 537—538.

"Impersonation" permits an unauthorized user to assume the identity of an authorized user by such means as using the authorized user's password or log-in code. Id.

A "logic bomb" is a computer program that executes upon the fulfillment of a certain set of conditions. Id. at 538—37. Perhaps the most famous of the logic bombs are those computer viruses that destroy data or programs whenever the calendar date is Friday the 13th. For example, on Friday, October 13, 1989, the international news media reported a computer virus that plagued the Royal National Institute for the Blind, a charitable institution in London, England. NBC Nightly News (NBC television broadcast, Oct. 13, 1989).

"Piggybacking" is the secret connection, via telephone line, of a hidden terminal to a user's terminal. S. Lipner, supra, at 537. Because the computer system cannot distinguish between authorized and unauthorized users a perpetrator can take advantage of a user's access to the computer, even when the user does not use his terminal. Id. at 537.

A "salami" is a method of embezzlement using a computer program that transfers small amounts of money, which the perpetrator hopes will go unnoticed, from numerous accounts into the perpetrator's account, accumulating a large amount of money. Id. at 533—34.

"Superzapping" is a method of altering computer data by using an International Business Machines (I.B.M.) computer systems tool that bypasses normal controls. Superzapping often does not require the use of normal computer program access procedures, such as logging into a journal, which would otherwise at least record the operator of the program or the data that was altered. Id. at 534—35.

A "trap door" is a facility within a computer program that allows authors or maintenance programmers to insert additional program instructions into a program in the event that the original program contains a problem that requires correction. Id. at 535—36. Misuse of trap doors can include modifying or destroying programs or data. Id.

A "trojan horse," for example, is a destructive program concealed within a useful program. Id. at 532—33. A rather devious example is an antiviral computer program, designed to detect computer viruses, but which itself carries a computer virus program. Highland, The Scourge of Computer Viruses, 240 Science 133 (Apr. 8, 1988) [hereinafter The Scourge].

18. McAfee, supra note 1, at 33. Three technical categories of computer viruses exist. Id. at 32. First are the boot infectors, viruses which copy themselves onto the sector or portion of the floppy or hard disk that stores the electronic memory containing the program used for booting or starting the system. Id. Next are system infectors, viruses that copy themselves onto system diskettes as they are inserted. Id. These viruses can affect such elements of the system as command interpreters, which translate computer language into the electronic signals that run the computer; keyboard, disk, and other data input devices; all printing functions; and transmission and reception of electronic memory storage. Id. Third are generic application infectors, viruses that copy themselves onto application programs such as spreadsheets, word processors, or other user-oriented programs. Id. After the infected application program is executed, these viruses can search for other programs in the system to which they can attach. Id. Most system infectors or generic application infectors simply attach or copy themselves onto programs while some boot infectors viruses replace the original program with the program of the virus. Id. at 33.
contain the virus; because many host programs do not have enough internal space to hold large virus programs, internal viruses spread slowly.\(^{19}\) External viruses are easier to spread. They usually increase the program's size in the memory and often show the newly increased size in the computer directory.\(^{20}\) External viruses remove a portion of the host program and replace it at the end of the program, restoring the program to its original format after execution of the virus.\(^{21}\) Although external viruses are more easily detected, their relative ease of attachment makes them easier to spread and, therefore, more prevalent.\(^{22}\)

B. History of Computer Viruses

The formal study of computer crime began in 1971.\(^{23}\) Numerous reports, articles and books followed the first national conference on computer abuse in 1973.\(^{24}\) Increasing cases and activities of the F.B.I. Academy, the National District Attorneys' Association Economic Crime Project, local F.B.I. offices, and the national College of District Attorneys have contributed to the literature available in this field.\(^{25}\) The F.B.I. established computer crime training courses for its agents in 1976 and for other agencies in 1978.\(^{26}\) Media events, such as a 60 Minutes presentation of an electronic funds transfer to Dan Rather,\(^{27}\) and the movie War Games,\(^{28}\) have caused some sensationalism.\(^{29}\)

The use of computer viruses began in the 1970's.\(^{30}\) Initial uses were beneficial; early computer viruses aided computer security

---

19. Id. at 34.  
20. Id. at 31—32.  
21. Id. at 33.  
22. Id. at 34.  
23. S. LIPEZ, supra note 17, at 515.  
24. Id.  
25. Id.  
26. Id.  
28. War Games (United Artists Corp. 1983).  
29. Richard C. Hollinger and Lonn Lanza-Kaduce of the University of Florida theorize that media distortion and sensationalism caused the outbreak of computer crime legislation, and that the statutes address the media's portrayal of the problem, rather than the problem itself. Hollinger and Lanza-Kaduce, The Process of Criminalization: The Case of Computer Crime Laws, 26 CRIMINOLOGY 101, 106—07 (Feb. 1988) [hereinafter Hollinger]. The authors describe computer law as a unique area of criminal law because the substantive law is in its infant stages and is primarily statutory in origin. Id.  
firms in tracking illegally copied programs. These early viruses were created to deter "pirating," the unauthorized use of copyrighted software.

Later uses of computer viruses were harmful and malicious. By 1985, magazines began reporting the use of "logic bombs" to vandalize data and make it inaccessible to the user. In 1988, Robert Tappan Morris, the son of a chief scientist at the National Security Agency's Computer Security Center, started a highly publicized virus that spread through two major computer networks connecting the California Institute of Technology, N.A.S.A.'s Ames Research Center, Stanford University, Harvard University, and Princeton University, among others. In 1989, John McAfee, director of the Computer Virus Industry Association in Santa Clara, California, received estimates of 10,000 virus infections per month, twice the 1988 rate. More than ten new virus infection strains, non-existent in 1988, appeared in the two months preceding Friday, October 13, 1989.

The development of technology, computer crime, and computer viruses is challenging the pace of criminal law development. Gross receipts of data processing companies increased from two billion dollars to ten billion dollars between 1972 and 1982. Between 1983 and 1985 the number of electronic bulletin board services providing access codes for users to charge phone bills to other parties increased from 125 to 1,000. Because of the speed of computer execution, some criminals commit crimes on computers in less than three milliseconds. According to some estimates, proceeds from

31. Id. at 628.
32. Id. at 629. For examples of recreational uses of viruses in controlled computer games, see Branchom, Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, 16 Rutgers Computer & Tech. L.J. 1, 9–10, and n.42 (1990). For illustrations of some newsworthy and fascinating computer virus incidents, see id. at 6–24.
34. Wilcox, supra note 2.
35. Friday the 13th PC Virus May Be All Hype and No Byte, ATLANTA J., Oct. 13, 1989, at A21, col.1 [hereinafter Friday the 13th].
36. Id.
37. S. Lipner, supra note 17, at 582.
40. S. Lipner, supra note 17, at 512–13.
computer crimes may range from ten thousand dollars to four hundred fifty thousand dollars.\textsuperscript{41}

Computer criminal law is still in its infancy.\textsuperscript{42} By February 1986, only seventy cases of computer crime had been tried in the United States.\textsuperscript{43} One poll of Fortune 500 companies showed that approximately three-quarters of the people in states with computer crime laws were unfamiliar with any such laws.\textsuperscript{44} A business that is afraid of harming its image may hesitate to report computer crime.\textsuperscript{45} In many states, the language of the existing statutes has failed to include computer acts that ought to be criminalized.\textsuperscript{46} In some cases, prosecutors have been unaware of existing computer crime laws.\textsuperscript{47} Even if state and federal officials are aware of the computer crime statutes, prosecution of computer crime often requires special expertise because of the technology involved.\textsuperscript{48}

\textbf{C. Development of Antiviral Programs}

The outbreak of computer viruses created a new industry—antiviral software.\textsuperscript{49} Antiviral programs take advantage of the weaknesses or common attributes of all viruses.\textsuperscript{50} Viruses can only infect programs; they cannot infect data files.\textsuperscript{51} Viruses must locate themselves in specific parts of host programs, but these locations will vary from program to program.\textsuperscript{52} The virus program must be in a position of control before it can execute.\textsuperscript{53} Further, the virus must change the system in some observable way.\textsuperscript{54} Virus protection programs may protect either computer software or hardware.\textsuperscript{55}

\begin{flushleft}
\textsuperscript{42} Computer Crime Statutes, supra note 41, at 223.
\textsuperscript{43} States Enact Legislation, supra note 39.
\textsuperscript{44} First Annual Report, supra note 38, at 30.
\textsuperscript{46} Gemignani, supra note 33, at 56—57.
\textsuperscript{47} Computer Crime Statutes, supra note 41, at 215.
\textsuperscript{48} Gemignani, supra note 33, at 56.
\textsuperscript{49} McAfee, supra note 1, at 34.
\textsuperscript{50} Id.
\textsuperscript{51} Id. at 34—35. Once they are in the programs, however, viruses can alter or destroy data files.
\textsuperscript{52} Id. at 36.
\textsuperscript{53} Id. at 35.
\textsuperscript{54} Id. at 36.
\textsuperscript{55} Highland, An Overview of 18 Virus Protection Products, 7 COMPUTERS AND SECURITY 156, 159 (Apr. 1988).
\end{flushleft}
Three types of antiviral programs prevent, detect, or identify computer viruses. These types are: infection protection programs, virus detection programs, and virus identification programs.\textsuperscript{56} Infection protection programs warn of viruses entering the system, but they can create false alarms.\textsuperscript{57} Even antiviral (or protection) programs can be fooled by sophisticated viruses that write directly to hardware, or bypass the usual access system of communication within the computer.\textsuperscript{58} Infection protection programs cannot prevent boot segment infections,\textsuperscript{59} because the computer must execute the boot or start-up program\textsuperscript{60} before the preventive program can function.\textsuperscript{61} Some virus programs can theoretically gain control over the entire computer.\textsuperscript{62}

The other two antiviral program types, virus detection programs and virus identification programs, function after the virus executes.\textsuperscript{53} Virus detection programs locate infection traces\textsuperscript{64} or characteristics by self-checking every program for changes, or by comparing every program to the log program as it was originally loaded into the system.\textsuperscript{65}

Finally, virus identification programs search for, deactivate, and remove known viruses from the system; these programs cannot discover unknown virus strains, however.\textsuperscript{66} Neither virus detection programs nor virus identification programs can prevent new virus strains from activating before they are detected. Once computer technicians discover the new viruses, they can create new antiviral programs to combat the harm.\textsuperscript{67}

II. STATE COMPUTER CRIME STATUTES

States have adopted many different statutory approaches to the general problem of computer crime.\textsuperscript{68} Of the forty-nine states with

\begin{itemize}
\item 56. McAfee, supra note 1, at 37.
\item 57. Id.
\item 58. Id.
\item 59. Id. A boot segment infection is the harm caused by a virus to the program that starts the computer. Id. See supra note 18.
\item 60. Id. During the execution of the start-up program, the virus can also execute. Id.
\item 61. Id. at 37–38.
\item 63. McAfee, supra note 1, at 37.
\item 64. Id.
\item 65. Id.
\item 66. Id. at 39.
\item 67. Id. Winn Schwartzan, a Nashville software engineer, estimates that 50,000 copies of his antiviral program were sold in the week preceding Friday, October 13, 1999, grossing over $1 million. Friday the 13th, supra note 35, at A21, col.1.
\item 68. Guide to the Prosecution of Telecommunication Fraud for the Use of Computer Crime
\end{itemize}
computer crime laws, only five, California, Illinois, Maine, Minnesota, and Texas, specifically address the spread of computer


any set of computer instructions that are designed to modify, damage, destroy, record or transmit information within a computer, computer system, or computer network without the intent or the permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.


inserts or attempts to insert a "program" into a computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by the computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of a computer which accesses or which is accessed by such "program".


71. In 1989 the Maine legislature enacted a statute which prohibits anyone from "[i]ntentionally or knowingly introducing or allowing the introduction of a computer virus into any computer resource, having no reasonable ground to believe that the person has a right to do so." Me. Rev. Stat. Ann. tit. 17-A, § 433.1(C) (Supp. 1990). The statute defines "computer virus" as

any computer instruction, information, data or program that degrades the performance of a computer resource; disables, damages or destroys a computer resource; or attaches itself to another computer resource and executes when the host computer program, data or instruction is executed or when some other event takes place in the host computer resource, data or instruction.


72. The Minnesota legislature amended its computer crime statute in 1989 to prohibit the distribution of a "destructive computer program." Minn. Stat. Ann. § 609-88, Subd. 1(c) (West Supp. 1991). The statute defines "destructive computer program" as a computer program that performs a destructive function or produces a destructive product. A program performs a destructive function if it degrades performance of the affected computer, associated peripherals or a computer program; disables the computer, associated peripherals or a computer program; or destroys or alters computer programs or data. A program produces a destructive
viruses. Although the statutes lack uniformity, the divergence of approaches may lead to the discovery of the most effective statutory approach. No two states have enacted identical statutes, but some simple patterns exist. The patterns may best be observed by studying the definitions of the substantive offenses and the penalties.

product if it produces unauthorized data, including data that makes memory unavailable; results in the unauthorized alteration of data or computer programs; or produces a destructive computer program, including a self-replicating computer program.


73. In 1989, the Texas legislature passed a statute that prohibits anyone from knowingly and without authorization "insert[ing] or introduc[ing] a computer virus into a computer program, computer network, or computer system." **Tex. Penal Code Ann. § 33.03(a)(6) (Vernon Supp. 1990).** The statute defines a "computer virus" as an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself and to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

**Tex. Penal Code Ann. § 33.01(b) (Vernon Supp. 1990).**

74. The following provisions illustrate the diversity of these statutes.


75. For two somewhat different views on state computer crime statutes, *compare* Branscomb, supra note 32 at 61, App. A; with Jurkat, supra note 68 at 520—44.
A. Defining the Substantive Offenses

States employ four general approaches when defining substantive computer crimes. First, most states have general computer crime statutes prohibiting several types of computer misconduct.\textsuperscript{76} Second, a few states specifically address computer viruses in their statutes.\textsuperscript{77} Third, a couple of statutes simply modify traditional crime statutes, such as those prohibiting theft, to include such intangibles as computer time or computer services.\textsuperscript{78} Finally, several states combine the three statutory approaches.\textsuperscript{79}

Two common problems mar many state computer crime statutes. First, many of the statutes are underinclusive in scope. A majority of the state computer crime statutes do not address computer viruses specifically.\textsuperscript{80} The most common general


\textsuperscript{77} See The five computer virus statutes cited supra, notes 70—73.\textsuperscript{78} MASS. GEN. LAWS ANN. ch. 266, § 30 (West Supp. 1990); OR. REV. CODE ANN. § 2901.01(2), (L)-(M) (Anderson Supp. 1989).


\textsuperscript{80} See supra note 69-73 and accompanying text.
computer misconduct provisions prohibit unauthorized access, unauthorized alteration or destruction of data, access with intent to steal, access for fraudulent purposes, unauthorized
interception or disclosure of data,\textsuperscript{85} and intentional unauthorized disruption of computer services,\textsuperscript{86} but these provisions do not mention the spreading of computer viruses. Most of the statutes prohibit general computer misconduct but do not address the specific situation in which a person creates a self-replicating program and either gives that program to someone else or transmits the program in a computer which then spreads the virus over a computer network or computer communications link.\textsuperscript{87}

Second, many state computer crime statutes, including those that specifically address the spreading of computer viruses, are vague or overbroad. Many of these statutes prohibit various types of “unauthorized” computer misconduct,\textsuperscript{88} but only a few define “authorization.”\textsuperscript{89} This means that computer crime statutes include

\begin{verbatim}
ANN. § 439.8451(1a); LA. REV. STAT. ANN. § 14:73.5.A(1); MICH. COMP. LAWS ANN. § 152.794;
MINN. STAT. ANN. § 609.88. Subd.1(b); MISS. CODE ANN. § 95-45-301(a); MO. ANN. STAT. § 569.055.2; MONT. CODE ANN. § 45-6-511(1b); NEV. REV. STAT. ANN. § 205.4765.4; N.J. REV.
STAT. § 2C:20-25(b); N.M. STAT. ANN. § 30-45-3; N.C. GEN. STAT. § 14-454(a)(1); N.D. CENT.
CODE § 12.1-66.1-08.1; OKLA. STAT. ANN. tit. 21, § 1583.2; OR. REV. STAT. § 164.377(2); 18 PA.
CONS. STAT. ANN. § 3933(a)(1); R.I. GEN. LAWS § 11-52-211; S.C. CODE ANN. § 16-15-501(1a);
S.D. CODIFIED LAWS ANN. § 34-43B-13(b); TENN. CODE ANN. § 39-14-602(a); UTAH CODE ANN. § 
76-6-7030(b); VA. CODE ANN. § 18.2-162.3; W.VA. CODE § 61-3C-5; WIS. STAT. ANN. 943.702(b);
WYO. STAT. § 6-3-502(b)(ii).
\end{verbatim}

\begin{verbatim}
85. ALA. CODE § 13A-5-102(c); ARIZ. REV. STAT. ANN. § 13-2316(b); CONN. GEN. STAT. ANN. § 
53a-251(e)(2)(b); DEL. CODE ANN. tit. 11 § 935(1); FLA. STAT. ANN. § 815.04(3); KAN. STAT.
ANN. § 21-3752(a); LA. REV. STAT. ANN. § 14:73.5.A(2); MISS. CODE ANN. § 95-45-501; MO. 
ANN. STAT. § 569.055.1(b); NEV. REV. STAT. ANN. § 205.4765.1; N.H. REV. STAT. ANN. § 
638:17IV(a); N.J. REV. STAT. § 2C:20-25(d); N.Y. PENAL LAW § 156.30; OKLA. STAT. ANN.
tit. 21, § 1583.3; 18 PA. CONS. STAT. ANN. § 3933(a)(3); TEX. PENAL CODE ANN. § 33.02(b); UTAH
CODE ANN. § 76-6-7031(1), (2); VA. CODE ANN. § 18.2-162.4; WIS. STAT. ANN. 943.702(a); WYO.
STAT. § 6-3-504(a)(iii).
\end{verbatim}

\begin{verbatim}
86. CAL. PENAL CODE § 502(c)(5); CONN. GEN. STAT. ANN. § 53a-251(d); DEL. CODE ANN. tit.
11 § 934; FLA. STAT. ANN. § 815.06(1); O.C.G.A. § 16-9-90(b)(2); ILL. ANN. STAT. ch. 38, para.
16D-4; LA. REV. STAT. ANN. § 14:73.4.A(2); MD. ANN. CODE art. 27 § 146(c)(2); MISS. CODE
ANN. § 95-45-501(a); MO. ANN. STAT. § 569.099.102; NEB. REV. STAT. §§ 28-1344(1), -1349(2);
NEV. REV. STAT. ANN. § 205.477.1; N.H. REV. STAT. ANN. § 638:17(IID); N.C. GEN. STAT. § 14-
456; OKLA. STAT. tit. 21, § 1583.1; 18 PA. CONS. STAT. ANN. § 3933(2); S.C. CODE ANN.
§ 16-16-203(b); TEX. PENAL CODE ANN. § 33.03(a)(XII) (interception to gain a business
advantage); UTAH CODE ANN. § 76-6-7034(a); WASH. REV. CODE ANN. § 9A.52.120; W.VA. CODE
§ 61-3C-5; WYOMING. STAT. § 6-3-504(a)(iii).
\end{verbatim}

\begin{verbatim}
87. See supra note 69—73 and accompanying text. See also McAfee, supra note 1, at
29—40.
88. See supra note 81, 82, 85 and 86 and accompanying text.
89. Six states seem to put the burden (in part at least) on the computer owner to define
“authorization”. CAL. PENAL CODE § 502h (West 1991) (An exception to the definitions of
computer crimes exists for any person “acting within the scope of his or her lawful
consent of a person; which may include an employee’s job description to use said person’s
\end{verbatim}
an undefined term as an element of the statutorily defined computer crimes. Consequently, to convict computer criminals, prosecutors must prove the existence of this undefined lack of authorization.

Presumably, computer owners or their agents could define the scope of "authorization" or permission they wish to give to computer users. The owners should then notify the computer users of the scope of permissive computer use. Otherwise, courts have difficulty when they attempt to define the scope of the permission. This lack of notice may cause the statutes to be overbroad and subject to constitutional attack.

B. Classification of Penalties

The statutes also delineate different penalties for computer crimes. Some statutes provide that all computer crimes are

---

computer, computer network, computer program, computer software, computer system property or services." *Id.* Under O.C.G.A. § 16-9-92(11), "[w]ithout authority" includes the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network." *Id.*


§ 16D-7. Rebuttable Presumption-without authority. In the event that a person accesses or causes to be accessed a computer, which access requires a confidential or proprietary code which has not been issued to or authorized for use by that person, a rebuttable presumption exists that the computer was accessed without the authorization of its owner or in excess of the authority granted.

*Id.*

Under N.Y. Penal Law § 156.00(6)(a)—(c) (McKinney 1988). Notice may be given by:

(a) giving actual notice in writing or orally to the user; or

(b) prominently posting written notice adjacent to the computer being utilized by the user; or

(c) a notice that is displayed on, printed out on or announced by the computer being utilized by the user. Proof that the computer is programmed to automatically display, print or announce such notice ... shall be presumptive evidence that such notice was displayed, printed or announced.

*Id.*

*Va. Code Ann. § 18.2-152.2* (Supp. 1990). ("A person is 'without authority' when he has no right or permission of the owner to use a computer, or, he uses a computer in a manner exceeding such right or permission." *Id.*) *W.Va. Code § 61-3C-3(b)* (Supp. 1990). ("Authorization means the express or implied consent given by a person to another to access or use said person's computer, computer network, computer program, computer software, computer system, password, identifying code or personal identification number." *Id.*)

90. See supra note 89.


The failure to define "authorization" exposes these laws to attack on constitutional grounds of vagueness and overbreadth. Computer professionals often modify programs and data to conform to their particular needs; they need to know what changes are authorized. Statutory language must be clear enough to protect this innocent, unauthorized use from criminal penalty.

92. Three statutes include in their penalty provisions forfeiture of computer equipment.
felonies.93 Others classify some offenses as felonies and other offenses as misdemeanors.94 Some states grade the severity of the penalty according to the amount of damage the crime causes.95 Other states grade severity according to the type of offense committed.96 Still other states do both, basing the penalty for some crimes upon the type of offense and penalizing the type of offense according to the amount of damage the crime causes.97


California requires a court to consider two mitigating factors in fixing the penalty. Cal. Penal Code § 502.01 (West Supp. 1991). First, a sentencing court must consider the level of prohibition on access to the computer. Cal. Penal Code § 502.01(c). Second, a court must consider alternative sentencing, “including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.” Cal. Penal Code § 502.02 (West Supp. 1991).


1991] COMPUTER VIRUSES

The penalty provisions in most of the state computer crime statutes may be unconstitutionally vague. Although most of the statutes grade the severity of the penalty according to the amount of damage the crime causes, few statutes include the intangible elements courts could instruct juries to include when calculating the amount of damage upon which the penalty is based. For example, few statutes take into account whether the relevant damage includes intangibles such as lost computer time, lost data, or lost anticipated profits. Until the case law develops, the penalty for a given crime will be uncertain because the method of calculating the damages remains undefined.

State computer crime statutes prohibit several types of computer misconduct. Many statutes fail to address computer viruses specifically, fail to define "authorized" conduct, and fail to provide a means for calculating damages, or for applying a penalty. These failings could cause the statutes to be found under-inclusive and overbroad. Theoretically, courts can fill these gaps by interpreting the legislative intent of the statutes. Without creative judicial interpretation, however, most state computer crime statutes cannot be applied to prohibit the spread of computer viruses.

III. STATE CASE LAW

Research of state case law reveals no reported opinions that apply computer crime statutes to computer viruses. The reported cases show that courts have experienced difficulties when attempting to apply these statutes to other types of computer

16-20(1) — (4); TENN. CODE ANN. § 39-14-602; TEX. PENAL CODE ANN. §§ 33.02, .03; UTAH CODE ANN. § 76-6-703; VA. CODE ANN. §§ 18.2-152.3 to -152.7; WASH. REV. CODE ANN. § 9A.46.100; WIS. STAT. ANN. §§ 943.70(2), (3).
98. See supra notes 95—97 and accompanying text.
99. CONN. GEN. STAT. ANN. § 53a-259; DEL. CODE ANN. tit. 11, § 937(b); IOWA CODE ANN. § 716A.1; MINN. STAT. ANN. § 609.87. Subd. 10; MONT. CODE ANN. § 45-2-101(6)(a)(iH); N.H. REV. STAT. ANN. § 638:18(V); N.J. REV. STAT. § 2C: 20-24; W.VA. CODE § 61-3C-3(o), (q).
100. But see supra note 99. The eight statutes which define "value" include the fair market value of property and services, the cost to replace data, and lost profits, to the extent that the fair market value of computer time, data or software, includes profits. Supra note 99. West Virginia defines "value" to mean "having any potential to provide any direct or indirect gain or advantage to any person." W. VA. CODE § 61-3C-3(o) (Supp. 1990).
101. See supra note 80—91 and accompanying text.
abuse. First, the failure to include computer services in the definition of property can prevent a conviction. Second, imprecise legislative drafting may omit some types of computer misconduct. Third, traditional crime statutes require elements of proof that may not exist in a case of computer abuse. The following cases do not involve computer viruses, but they illustrate these difficulties with respect to general computer crime statutes.

A. Defining Computer Services

In *Lund v. Commonwealth*, the state of Virginia charged the defendant, Lund, with grand larceny for using computer time and services without authorization. Lund needed access to the Virginia Polytechnic Institute and State University (VPI) computer system to work on his Ph.D. dissertation. Instead of obtaining authorization, he accessed the computer with the help of another student. The computer center's director estimated that Lund had used over $25,000 worth of unauthorized computer services.


104. Lund v. Commonwealth, 222 S.E.2d 745 (1977). "Some jurisdictions have amended their criminal codes specifically to make it a crime to obtain labor or services by means of false pretenses ... We have no such provision in our statutes ... We [also] hold that labor and service and the unauthorized use of ... [computers] cannot be construed to be subjects of larceny ..." Id. at 748.

In Virginia computer services do not constitute property within the meaning of the criminal statutes prohibiting larceny and obtaining property by false pretense. *Id.* The *Lund* court also noted Virginia's similarity to the common law in this respect. *Id.* In 1984 the Virginia legislature enacted 1984 Va. Acts 751 (codified at VA. CODE ANN. §§ 18.2-152.1 to -152.14 (Supp. 1990)).

105. People v. Weg, 450 N.Y.S.2d 957 (1982). "Although a court must not be overly technical in interpreting penal provisions, penal responsibility cannot be extended beyond the fair scope of the statutory mandate ..." *Id.* at 961 (quoting People v. Case, 396 N.Y.S.2d 841, 365 N.E.2d 872 (1977)). The *Weg* court also stated, "Unless [the statutory basis upon which the defendant was charged] is amended, it will apply only to unauthorized tapping into a computer whose service is for hire." *Weg*, 450 N.Y.S.2d at 961.

106. State v. McGraw, 490 N.E.2d 552 (Ind. 1986). The Supreme Court of Indiana held in *McGraw* that a conviction for unauthorized computer use, based upon a general theft statute, must be reversed because "[t]here was no evidence presented from which the intent to deprive, an essential element of the crime, could be inferred." *Id.* at 555. See also *Gemignani, supra* note 33, at 60–61.


109. *Id.*

110. *Id.* at 747.

111. *Id.*
A subsequent investigation turned up many computer cards and printouts in his apartment. Lund argued that these items were neither stolen nor worth more than the $100 statutory requirement for larceny. He also contended that the grand larceny requirement—that one obtain goods and chattels—does not include computer time and service.

The Virginia Supreme Court accepted Lund’s argument, reversed his conviction, and quashed the indictment. The court held that strict statutory construction of the Virginia larceny statute excluded computer time and service from the interpretation of “goods and chattels.” The court further stated that the crime of false pretenses requires a “taking and carrying away,” which is impossible with computer time and service. Although some states include labor and services in their false pretenses statutes, Virginia does not. The Virginia legislature responded to the decision by enacting a statute that prohibits the conduct at issue in Lund.

B. Precision in Legislative Drafting

In People v. Weg, the state of New York charged Weg with theft of services from his employer, the New York City Board of Education. Weg had used the Board’s computer for his own benefit without authorization. The information alleged violation of a New York statute that prohibits the unauthorized use of an employer's business equipment “with intent to derive a commercial [benefit].” Weg moved to dismiss, arguing that the prosecution had failed to state a crime and had not factually supported each element of the crime charged.

The Criminal Court of the City of New York, Kings County, dismissed the charge, holding that the statute proscribed the use

112. Lund, 232 S.E.2d at 747.
113. Id.
114. Id.
115. Id. at 749.
116. Lund, 232 S.E.2d at 748. “Where there is no market value of an article that has been stolen, the better rule is that its actual value should be proved ... Here ... the director of the computer center stated that the printouts had no more value than scrap paper.” Id.
117. Id.
118. Id.
119. Gemignani, supra note 33, at 62.
120. 450 N.Y.S.2d 957 (N.Y. City Crim. Ct. 1982).
121. People v. Weg, 450 N.Y.S.2d at 958.
122. Id.
123. Id.
of commercial equipment, which did not include the Board of Education's computers.\textsuperscript{124} The court interpreted the statute to require an intent to receive commercial gain,\textsuperscript{125} and found that a contrary holding would criminalize the actions of thousands of employees who make personal use of their employers' equipment.\textsuperscript{126} The court also stated that the statute would have been clearer if it had stated explicitly the requirement of intent to receive commercial gain.\textsuperscript{127} The court referred to the computer statutes of other states, and suggested a possible need for legislative action regarding computer crime.\textsuperscript{128}

C. Applying Traditional Criminal Statutes to Computer Crime

In State v. McGraw,\textsuperscript{129} Indiana charged McGraw with theft of "the use of computer services."\textsuperscript{130} McGraw had previously worked for the Indianapolis Department of Planning and Zoning, where he had used his employer's leased computer service for his private business.\textsuperscript{131} His employer warned him to stop using the computer to maintain his own client lists, inventory control, and client letters and records\textsuperscript{132} and eventually fired McGraw for poor performance and unauthorized computer use.\textsuperscript{133} After McGraw persuaded a coworker to print out his computer files, the coworker reported the incident to a supervisor.\textsuperscript{134} Although the jury found McGraw guilty, the judge granted McGraw's motion to dismiss the charges because of the prosecution's failure to state an offense.\textsuperscript{135} The Indiana Court of Appeals reversed the trial court's decision and reinstated McGraw's conviction.\textsuperscript{136} McGraw then appealed to the Indiana Supreme Court.\textsuperscript{137}

\begin{enumerate}
\item Id. at 960.
\item \textit{Weg}, 450 N.Y.S.2d at 960.
\item Id. at 961.
\item Id.
\item Id. "Perhaps computers are a special type of expensive, commonly owned equipment, so subject to misuse that the legislature might wish to give their owners special protection ... Other legislatures have recently addressed this problem ... This court, however, may not create an offense." \textit{Id}.
\item New York later passed a computer crime statute which deleted the requirement of commercial gain. \textit{N.Y. PENAL LAW § 156.00 to .50} (McKinney 1988).
\item 459 N.E.2d 61 (Ind. App. 1984).
\item Id.
\item Id. at 62--63.
\item Id. at 63.
\item Id. at 63.
\item \textit{McGraw}, 459 N.E.2d at 63. The requested print-out was five inches thick. \textit{Id}.
\item Id.
\item Id. at 64.
\item Id. at 65.
\item 480 N.E.2d 552 (Ind. 1985).
\end{enumerate}
The Indiana Supreme Court again reversed McGraw’s conviction, construing the theft statute strictly against the state.\textsuperscript{138} The court found that McGraw did not intend to deprive the employer of anything; therefore, the intent element of the crime was not proven.\textsuperscript{139} The court compared McGraw’s unauthorized use of computer time to that of storing his personal belongings on a shelf at work.\textsuperscript{140}

These cases show three potential drawbacks with applying state computer crime statutes to cases of computer abuse. First, some aspects of computer crime, such as computer time and services, are intangible. Second, precision in legislative drafting is difficult. Innovation and technology continually make new forms of computer abuse possible. Computer crime defendants are likely to focus on imprecisely worded statutory sections which do not address new technology. Third, prosecuting computer abuse under traditional crime statutes is difficult. The law of computer viruses, yet in its infancy,\textsuperscript{141} seems to have inherited these drawbacks.

IV. FEDERAL COMPUTER CRIME STATUTES

Although as many as forty federal computer crime statutes address specific computer activities, no federal statutes prohibit the spread of computer viruses among privately owned computer systems.\textsuperscript{142} Two Congressional acts prohibit computer fraud: the

\textsuperscript{138} Id.
\textsuperscript{139} Id. at 554. The court reasoned that, in cases in which the employer suffered no deprivation, the state was required to show evidence of an intent to deprive, which the state did not do. Id.
\textsuperscript{140} Id. "Defendant has likened his conduct to the use of an employer's vacant bookshelf, for the temporary storage of one's personal items, and to the use of an employer's telephone for toll-free calls. The analogies appear to us to be appropriate." Id.
\textsuperscript{141} See Hollinger, supra note 29 at 106-107.
\textsuperscript{142} C. SHERMAN, H. SANDISON, M. GUREN, COMPUTER SOFTWARE PROTECTION LAW 317—5 to —8 (1989) [hereinafter C. SHERMAN]. But cf. H.R. 55, 101st Cong., 1st Sess. (1989). [hereinafter H.R. 55]. Rep. Herger, on behalf of 32 congressman, introduced the Computer Virus Eradication Act of 1989 in the House of Representatives. The bill never passed. The bill would have made it a felony to insert instructions into a program the perpetrator knows or believes will cause harm to users of a computer running the program, or to people who rely on the computer's information processing, or to users of other computers. The bill would have required the state to show that the perpetrator provided the program, or provided a computer with the program, to someone who did not know of the program's effects. H.R. 55, supra, at Sec. 2. The bill did not define "loss, expense or risk to health or welfare," terms that constitute the harm the inserter of a virus must intend to cause to violate the proposed law. The bill might even have prohibited a person from inserting a virus into his own computer for experimental purposes. See also Comment, The Computer Virus Eradication Act of 1989: The War Against Computer Crime Continues, 3 SOFTWARE L.J. 717 (1990).

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the 1984 Act) and the Computer Fraud and Abuse Act of 1986 (the 1986 Act). While both of these statutes address specific abuses of computers, neither protects private computers that are not engaged in interstate commerce or that do not provide access to records of financial institutions.

A. The 1984 Act

The 1984 Act was the first federal statute specifically intended to protect computers and computerized information. Under the 1984 Act, it is a felony to access computer data on nuclear weapons and materials, foreign relations, or national defense without authorization. Unauthorized computer access of the financial records of credit reporting agencies and financial institutions constitutes a misdemeanor. The 1984 Act also makes it a misdemeanor to gain unauthorized access to a financial institution's computer to modify data without authorization.

The legislative history of the 1984 Act shows that Congress and the President considered tougher computer crime bills but settled


145. C. Sherman, supra note 142, at 317–8. The law prohibits only computer crimes involving federal-interest computers or computers that provide access to financial records of financial institutions and “trafficking which affects interstate or foreign commerce.” 18 U.S.C. § 1030 (1988).


147. 1984 Act § 2102(a). The 1984 Act punishes “[w]henever- (1) knowingly accesses a computer without authorization or exceeds authorized access and by means of such conduct obtains information . . . [regarding] national defense or foreign relations . . . of information classified under . . . the Atomic Energy Act of 1954.” Id.

A felony carries a fine of up to $10,000, or twice the value of the illegally obtained information, a prison term of up to 10 years, or both. Id. A repeat felony offense is punishable by a fine of up to $100,000, or twice the value of the property obtained, 20 years imprisonment, or both. Id.

148. Id. The statute punishes one who intentionally, through unauthorized access, “obtains information contained in a financial record of a financial institution . . . of a consumer reporting agency on a consumer.” Id. Penalties for a first misdemeanor offense include a fine of not more than $5,000, or twice the value of the information obtained, a prison term of not more than one year, or both. Penalties for subsequent misdemeanors include a fine of not more than $10,000, or twice the value of the information obtained, a prison term of up to ten years, or both. Id.

149. Id. This section punishes anyone who “knowingly accesses a computer without authorization and uses, modifies, destroys or discloses information in or prevents authorized use of” a government computer. Id.
on the 1984 Act at the end of the Ninety-eighth Session.\textsuperscript{150} A 1978 bill had served as a model for other unpassed computer crime bills.\textsuperscript{151} Some of these bills would have prohibited fraudulent use of data, programs or computers, as well as intentional damage or unauthorized use of a computer.\textsuperscript{152} Others prohibited fraud involving access devices.\textsuperscript{153}

The original version of the 1984 Act, as passed by the House, prohibited unauthorized access of any computer affecting interstate commerce where the access resulted in either a gain or loss of at least five thousand dollars.\textsuperscript{154} In response, the Reagan administration proposed a broader bill which, in addition, would have prohibited altering or destroying computer data or programs involving computers in two or more states, or in one state and in a foreign country. The bill would also have eliminated the five thousand dollar minimum requirement.\textsuperscript{155} The administration's bill left the problem of intrastate activity to state legislation.\textsuperscript{156} A Joint Resolution covering continuing government funding contained the 1984 Act, which included only the computer systems for national security, credit and financial institutions, and the federal government.\textsuperscript{157} The Senate passed a substitute bill, but the House did not.\textsuperscript{158} The 1984 Act passed by both houses is a weaker version of the proposed bills and leaves access to private computers and computer networks unaffected.\textsuperscript{159}

The Justice Department has identified two weaknesses in the 1984 Act.\textsuperscript{160} First, sensitive data, such as corporate financial accounts, census information, and tax returns, receive no protection under the 1984 Act.\textsuperscript{161} Second, determining the effect of the

\textsuperscript{150} C. Sherman, supra note 142, at 317—12 to —15. The proposed law would have been known as the Federal Computer Systems Protection Act. Comparable bills were introduced in 1979, 1981, and 1983. Id.

\textsuperscript{151} Id. at 317—12 to —13. For a list of references discussing these bills see id. at 317—12, n.85.

\textsuperscript{152} Id. at 317—13.

\textsuperscript{153} Id.

\textsuperscript{154} Id. at 317—14, n.102.

\textsuperscript{155} Id. at 317—14 to —15.

\textsuperscript{156} Id. at 317—5.

\textsuperscript{157} Id.

\textsuperscript{158} Id.

\textsuperscript{159} Id.

\textsuperscript{160} Jurkat, supra note 68, at 518.

\textsuperscript{161} Id. at 518 n.50—51.
government’s use of a computer system affected by unauthorized access is difficult.\textsuperscript{162}

The 1984 Act may have two additional problems. Requiring prosecutors to prove that a wrongful act has affected the government’s computer operation could distract a jury from the actual issue of unauthorized access.\textsuperscript{163} Also, the 1984 Act does not define either “authorization” or “use.”\textsuperscript{164} As a result, the question remains whether the law prohibits the act of causing another to “use” the computer in a way the person accessing the computer may not.\textsuperscript{165}

\textbf{B. The 1986 Act}

The 1986 Act amends the 1984 Act.\textsuperscript{166} The 1986 Act prohibits the alteration or modification of data in financial institutions’

\begin{footnotesize}
\begin{enumerate}
\item[162.] \textit{Id.} at 518 n.53. The prohibited conduct must “affect [some] such government operation.” 1984 Act § 2102(a).
\item[163.] Jurkat, \textit{supra} note 68, at 518.
\item[164.] \textit{Id.}
\item[165.] \textit{Id.} at 517–18.
\item[166.] The legislative history of the 1986 Act includes reports of a number of other proposed bills on computer crime. C. Sherman, \textit{supra} note 142, at 317–15 to –16. The Justice Department proposed a bill and expressed three concerns about the other proposed bills. Jurkat, \textit{supra} note 68, at 518. First, failure to track the mail and wire fraud provisions allows defendants to argue inapplicability of case law based on those provisions. \textit{Id.} Second, failure to address electronic trespass allows defendants to argue that mere scanning of systems is permissible. \textit{Id.} Finally, requiring the state to prove that the wrongful act has affected interstate commerce could distract a jury from the issue of fraudulent conduct. \textit{Id.} The Justice Department bill did not pass, but the 1986 Act does contain a provision defining the phrase “exceeds authorized access.” 18 U.S.C. § 1030(e)(6) (1988). The 1986 Act became law when both the Senate and House passed identical bills. C. Sherman, \textit{supra} note 142, at 316–17.
\end{enumerate}
\end{footnotesize}
computers causing a loss of one thousand dollars or more. The Act also prohibits the modification of data that impairs medical treatment to individuals. In addition, the 1986 Act prohibits the fraudulent transfer of computer passwords or similar information that could aid unauthorized computer access on two alternative conditions. Either the transfer must affect interstate commerce or the password trafficking must permit a person to gain unauthorized access to a government computer.

Penalties under the 1986 Act are similar to those under the 1984 Act but include an intermediate level of punishment. The punishment for fraudulent, unauthorized access to a government computer is a fine or a prison term of up to five years. Altering or damaging data, causing a loss of at least one thousand dollars, and causing a modification or impairment of medical treatment have the same penalty. A second offense raises the maximum prison term to ten years.

The 1986 Act mirrors many of the weaknesses of the 1984 Act. Several loopholes exist in the statute. The statute does not address the alteration or destruction of computer data or programs, so long as the damage does not exceed one thousand dollars and does not affect medical care. A person who has accessed a

trespass offense and prohibited it in the statute. Id.

Tension exists between the need for authorized users, such as federal employees, to freely access government computers and the need to prohibit unauthorized access by others. Id. The Committee intended to allow each agency to develop a policy for regulating cases in which users whose original access was permissible gained access beyond their authorization. Id. The statute does not prohibit the conduct of federal employees who simply gain access beyond their authorization. Id. Because the Committee feared potential for an overbroad application of the crime "computer fraud," it included in the statute a requirement that the prohibited fraudulent activity integrally (rather than incidentally) involve computers. 18 U.S.C. § 1030(a)(4) (1988). S. REP. No. 99-432, supra, at 16. The mail and wire fraud laws, therefore, do not control computer fraud cases. Id.


173. Id.
174. Id.
175. Id.
176. C. SHERMAN, supra note 142, at 317—16.
computer with fraudulent intent and who has obtained nothing of tangible value may attempt to argue that she has not violated the letter of the statute.\textsuperscript{179} The statute permits a person to gain unauthorized access with intent to defraud, if only computer use is sought, despite the valuable processing time and electrical power such use may consume.\textsuperscript{180} Further, the statute may authorize fraud, since it prohibits only unauthorized access with the intent to defraud.\textsuperscript{181}

V. FEDERAL CASE LAW

Federal courts have neither interpreted nor applied the 1984 Act or the 1986 Act in a published opinion.\textsuperscript{182} The following decisions involving computer crime may provide some precedent for deciding computer virus cases that may arise, however.

A. Conversion of Data Versus Free Access to Information

In \textit{United States v. Lambert},\textsuperscript{183} the federal government charged the defendant with selling information obtained from the Drug Enforcement Administration in Washington, D.C.\textsuperscript{184} The information allegedly revealed a confidential list of informants and drug investigation records.\textsuperscript{185} The statute at issue, 18 U.S.C. section 641, prohibits conversion or unauthorized sale of "any record, voucher, money, or thing of value of the United States."\textsuperscript{186} The defendant argued that information on a computer is not a "thing of value" within the meaning of the statute;\textsuperscript{187} that the statute, if applicable at all, was unconstitutionally vague in that it provided no notice of what conduct it prohibited;\textsuperscript{188} and that the statute violated the first amendment.\textsuperscript{189}

Despite earlier cases holding that the statute prohibits only conversion of tangible property,\textsuperscript{190} the court found that reasoning

\textsuperscript{180} \textit{Computer Crime Statutes}, supra note 41, at 218—19.
\textsuperscript{181} Id. at 219.
\textsuperscript{182} Robert Morris was convicted in an unreported decision, leaving no opinion to serve as precedent for future cases. See supra note 3 and accompanying text.
\textsuperscript{183} 446 F. Supp. 890 (D. Conn. 1978).
\textsuperscript{184} \textit{United States v. Lambert}, 446 F. Supp. at 892.
\textsuperscript{185} Id.
\textsuperscript{186} Id. at n.1 (quoting 18 U.S.C. § 641 (1970)).
\textsuperscript{187} Id.
\textsuperscript{188} \textit{Lambert}, 446 F. Supp. at 892.
\textsuperscript{189} Id. at 896.
\textsuperscript{190} See \textit{Chappel v. United States}, 270 F.2d 274 (9th Cir. 1959) (reasoning derived from tort law led to the conclusion that 18 U.S.C. § 641 does not prohibit the taking of information).
based upon common law tort principles was unnecessary. The court followed the Supreme Court's holding in Morissette v. United States, which supports the position that 18 U.S.C. section 641 derives its authority from outside the common law. The court found merit in the government's argument that the computer information was of exceptional value.

In answer to the vagueness challenge, the court stated that a person of ordinary intelligence would probably interpret the term "record" to include information stored in a computer. The court acknowledged possible statutory interpretations that would violate the first amendment, but held that the statute withstood careful scrutiny because it balanced the pursuit of the government's interest in law enforcement against the rights of citizens to gain access to government information.

Analogizing Lambert to the criminal law of computer viruses, because government computer data represents innumerable hours of work, it is of inestimable value. If the unauthorized use of data within a government computer can be said to parallel the conversion of government information, Lambert supports the prohibition of electronic trespass. Under this same analysis, Lambert would also require computer crime laws to protect the freedom of access to information.

B. Computer Data as Property

In United States v. Seidlitz, the government charged the defendant with wire fraud. The defendant had resigned his job

194. Id.
195. Id. at 896.
196. Id. at 899--900.
197. These rules are specific and carefully constructed to take into consideration the government's interest in law enforcement and the right of various groups to government information. The risk that these rules might interfere with constitutionally protected activity is minimal at best. Therefore these provisions are neither vague nor overbroad on their face.
198. Id. at 900.
199. Lambert, 446 F. Supp. at 895.
200. Cf. id. at 896.
201. United States v. Seidlitz, 589 F.2d at 154--155. The company discovered that the defendant accessed its computer by telephone. Id. An internal computer detection system determined that someone was obtaining the source code, or program instructions, of the company's private software. Id.
as a supervisor of computer security for a computer service firm and later used confidential information gained through his employment to access the firm's computer by telephone without authorization. The computer service firm requested a trace of the unauthorized call, but the telephone company would not reveal the identity of the caller without a subpoena. When the firm's detection system later recorded another unauthorized access using the same identification, the telephone company again traced the call, but did not reveal the caller's identity until later in the F.B.I.'s investigation. The F.B.I. suggested using telephone company tracing equipment, which would allow the firm to determine who made the unauthorized access without revealing the contents of the call. Subsequent traces and executed search warrants showed that the defendant had acquired forty rolls of printouts of the firm's source code. The defendant challenged his conviction for wire fraud and argued for reversal, claiming that, by using the detection equipment, the telephone company had obtained the information necessary for the warrants illegally.

The Fourth Circuit Court of Appeals interpreted the federal wire fraud statute and found that the data obtained was the telephone company's property. The Fourth Circuit affirmed the conviction, holding that the private firm's use of the detection equipment was permissible. The court contrasted the facts of Seidlitz to a situation in which the government could manipulate a private agent to assist in conducting illegal surveillance. In Seidlitz, the company freely initiated and consented to the investigation. The Seidlitz court did not decide whether the computer service firm's original call traces violated the fourth amendment.

---

202. Id. at 154.
203. Id.
204. Id.
205. Seidlitz, 589 F.2d. at 155.
206. Id. A source document, containing the source code, is the original set of program instructions that "form the basis of every entry into the computer." See R.I. GEN. LAWS § 11-52-1 (Supp. 1989).
207. Seidlitz, 589 F.2d at 155.
209. Seidlitz, 589 F.2d at 160.
210. Id. at 158.
211. Id.
212. Id. Use of the detection equipment was permissible because employees of the company may "aid" to the utmost of their ability in the apprehension of criminals." Id.
213. Seidlitz, 589 F.2d. at 158 n.20.
The Seidlitz court applied the wire fraud statute to computer abuse, asserting that federal jurisdiction over interstate communications exists and that computer data is property. Seidlitz may also permit private investigations of computer crimes, such as the spreading of computer viruses.

C. Wire Fraud and F.C.C. Jurisdiction Over Computers

In United States v. Giovenzo the government charged the defendant with wire fraud and conspiracy to commit wire fraud. The defendant’s coconspirator sold tickets for TransWorld Airlines (TWA). The normal TWA sales procedure required the defendant to enter flight data for a ticket into a computer terminal, which transmitted the information from Pittsburgh to the main computer in Kansas City, Missouri. The computer in Kansas City transmitted the information back to the Pittsburgh airport terminal, and a printer produced a ticket package that included a credit card charge form, an auditor’s coupon, flight coupons, and the customer’s receipt. Although the actual sale was for cash, the coconspirator would then give the customer the charge form and keep the extra flight coupons, the auditor’s coupon, and the customer’s receipt. The defendant gave the passenger a boarding pass and collected the flight coupon to reassemble the packet, which the coconspirator would mark “void” and return to the accounting office. TWA’s auditors did not look for cash from the voided tickets, and the defendant split the sales money with the coconspirator. The defendant appealed his conviction, arguing that the Federal Communications Commission (FCC) had no jurisdiction over such private interstate communication networks.

The Third Circuit Court of Appeals affirmed the conviction, stating that, under its interpretation of the legislative history, Congress intended to prohibit all wire fraud derived from interstate

214. Id. at 152 and 153 n.1.
215. Id. at 160.
216. Id. at 158.
217. 637 F.2d 941 (3rd Cir. 1980).
218. United States v. Giovenzo, 637 F.2d at 942.
219. Id. at 942.
220. Id.
221. Id.
222. Id.
223. Id.
224. Id.
225. Id. at 943.
commerce, limited only by the police power left to the states.\textsuperscript{226} The defendant's fraudulent conduct required the use of interstate wire transmissions.\textsuperscript{227} The court compared TWA to a telephone user who, though not regulated by the FCC, may violate the statute by using interstate telephone lines to make fraudulent representations.\textsuperscript{228} Since computer viruses may be spread by interstate transmission of computer information via telephone wires, as in \textit{Gioveno}, the wire fraud statute arguably prohibits the spread of computer viruses, if such spread is fraudulent.\textsuperscript{229}

\section*{VI. Policy Considerations}

Policy concerns affecting the law of computer viruses include the free exchange of information, ethics, and difficulties in prosecution. First, free exchange of information, in addition to expediting rapid technological growth, provides one of the most powerful tools of fighting computer viruses.\textsuperscript{230} Second, the ethical considerations of computer users influence the security of computer systems and networks.\textsuperscript{231} Third, prosecution difficulties may permit defendants to find loopholes in the statutes intended to fight

\begin{thebibliography}{99}
\bibitem{226} Gioveno, 637 F.2d at 943. See, e.g., 1952 U.S. Code Cong. & Admin. News 2234.
\bibitem{227} Id. at 943--45, 944 n.4. Although TWA is not a "common carrier" within the meaning of the Federal Communications Act, the airline's use of interstate telephone lines placed the case under the Federal Communications Commission's (FCC) jurisdiction. \textit{Id.} at 943.
\bibitem{228} The Court noted:
\begin{quote}
While TWA is not itself a "common carrier" for purposes of FCC jurisdiction, it does not follow that TWA is therefore incapable of violating the wire fraud act through its use of interstate communication. TWA might be compared to a user of the telephone who, although he is not himself subject to regulation by the FCC, may nonetheless violate [18 U.S.C.] § 1343 by attempting to obtain money through false representations transmitted by means of interstate telephone.
\end{quote}
\textit{Id.} at 944 n.4.
\bibitem{229} 18 U.S.C. § 1343 (1988) states:
\begin{quote}
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretense, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, scheme, or artifice, shall be fined not more than $1,000 or imprisoned not more than five years or both.
\end{quote}
\textsuperscript{230} Id. at 943--44.
\bibitem{230} Rochlis and Eichin, \textit{With Microscope and Tweezers: The Worm from MIT's Perspective}, 32 Communications of the ACM 689 (June 1989) [hereinafter Rochlis]. During the Cornell virus attack, "[j]ust like MIT and Berkeley were able to collaborate in a meaningful manner because they never took themselves off the network." \textit{Id.} at 696.
\bibitem{231} Farber, \textit{Statement of Ethics}, 32 Communications of the ACM 688 (June 1989).
\end{thebibliography}
computer viruses and may allow the proliferation of computer viruses to go unpunished.  

A. The Free Exchange of Information

Strict prohibitions of computer misuse can adversely affect the free flow of information. The Freedom of Information Act (FOIA) requires federal agencies to make documents available to anyone upon request and to list appropriate indices in the Federal Register. Agencies may refuse to disclose requested documents available under one of the statute's exceptions, but federal courts have jurisdiction to review agency refusals to disclose. The FOIA requires agencies to publish upon request any information not included in the exceptions. Agencies must respond to FOIA requests within ten days and process appeals for denied requests within twenty days. Lawyers may not use the FOIA as a means to circumvent normal discovery procedures. The FOIA may also cause agencies to be more willing to disclose information voluntarily, perhaps because plaintiffs have been successful in suing for disclosure under the FOIA.

In 1974, Congress passed the Privacy Act, which prevents an agency from releasing certain private information of citizens without an FOIA request. Also, if such information falls under one of the FOIA exceptions, an agency may not disclose the information. The FOIA and the Privacy Act penalize agencies for improper disclosure of information but do not penalize them for improper withholding of information. Thus, an incentive exists for an agency not to disclose information.

225. Id.
226. The exceptions include such information as national security, internal personnel rules, any statutory exception with an ascertainable standard for withholding of information, confidential trade secrets or financial status, inter-agency or intra-agency memos or letters, and personnel and medical files. 5 U.S.C. § 552(a), (b) (1982).
228. 5 U.S.C. § 552(b) (1982).
233. Id.
236. Id.
Unfortunately, computer crime statutes, including virus provisions, could adversely affect the free exchange of information.\textsuperscript{247} To avoid unlawful computer access, agencies may claim an additional incentive not to disclose information in response to FOIA requests.\textsuperscript{248} Computer crime restrictions could, therefore, discourage the disclosure of otherwise valid FOIA requests.\textsuperscript{249} Similarly, the private sector has a decreasing interest in exchanging information as the computer crime laws become stricter.\textsuperscript{250} Free exchange of information may be critical, though, in attacking computer crime.\textsuperscript{251}

B. Ethics

Ethics is another important policy concern in computer crime law.\textsuperscript{252} Focusing on ethics in computer education could help alleviate the spread of computer viruses.\textsuperscript{253} Such organizations as the Division Advisory Panel of the National Science Foundation's Division of Networking and Communications Research and Infrastructure,\textsuperscript{254} the Massachusetts Institute of Technology's Athena Project,\textsuperscript{255} the Internet Activities Board,\textsuperscript{256} and the Computer Professionals for Social Responsibility\textsuperscript{257} have published codes or statements of ethics. In published statements of ethics, these organizations have condemned or discouraged several acts, including: unauthorized access to the files of others,\textsuperscript{258} over-reliance on computers,\textsuperscript{259} disruption of computer networks,\textsuperscript{260} and conduct that wastes

\textsuperscript{247} Id.
\textsuperscript{248} Id. See 131 Cong. Rec. S2728-29 (Mar. 7, 1985).
\textsuperscript{249} C. Sherman, supra note 142, at 317-17.
\textsuperscript{250} For a contrasting view, see id. “[T]he 1984 legislative history makes it clear that the purpose of the [1984 Act] is to punish and deter computer trespassers .... Untoward results are ... not a necessary result or implication of the Act.” Id.
\textsuperscript{251} Rochlis, supra note 230, at 696.
\textsuperscript{252} Computer Viruses and the Law, supra note 30, at 640.
\textsuperscript{253} Id.
\textsuperscript{254} Farber, supra note 231, at 688.
\textsuperscript{255} Saltzer, Statement of Ethics, 32 COMMUNICATIONS OF THE ACM 704 (June 1989). “Project Athena has assumed that one of its responsibilities is to open a discussion of ethical use with its user community.” Id.
\textsuperscript{256} Cert, Statement of Ethics, 32 COMMUNICATIONS OF THE ACM 710 (June 1989). “Negligence in the conduct on Internet—wide experiments is both irresponsible and unacceptable.” Id.
\textsuperscript{257} Chapman, Statement of Ethics, 32 COMMUNICATIONS OF THE ACM 699 (June 1989). “We hope [the Cornell virus] will provoke long overdue public discussion about the vulnerabilities of computer networks, and the technological, ethical and legal choices we must address.” Id.
\textsuperscript{258} Saltzer, supra note 255.
\textsuperscript{259} Chapman, supra note 257.
\textsuperscript{260} Farber, supra note 231.
computer resources, including both people and equipment. At the same time, these organizations encourage the free exchange of ideas, including the publication of known weaknesses; the establishment of clear, effective computer-use policies, including enforcement through disciplinary measures; and personal accountability. Given the number of reported computer virus attacks, the effect of these ethical statements in preventing the spread of computer viruses is as yet unproven.

C. Problems for Prosecutors

Effective prosecution of computer crimes faces many challenges. Only a small percentage of the computer crime incidents investigated are prosecuted. A survey of prosecutors showed that some did not know that their states had computer crime statutes. Also, many prosecutors depended upon traditional statutes because the penalties were tougher than those in the computer crime statutes. In addition, victims may be uncooperative and prosecutors, grand juries, and courts may be unversed in computer technology.

VII. Diagnosis and Prescription

A. Diagnosis

Although the media may have sensationalized computer viruses unduly, computer users are genuinely threatened. Viruses can destroy equipment, programs, and data. If a virus were to infect an extensive medical computer network, for example, it could place human life at risk. Although national security computer systems are heavily protected, they may be vulnerable to a computer virus. Computer viruses could cause devastating harm.

261. Cerf, supra note 256.
262. Chapman, supra note 257.
263. Farber, supra note 231.
264. Chapman, supra note 257.
265. Friday the 13th, supra note 35. In 1989, computer viruses were reported at a rate of 10,000 per month. Id.
267. Id.
268. Id. (citing S. Nycum & D. Parker, Prosecutorial Experience with State Computer Crime Laws 33 (1986)).
269. Id.
Present methods of fighting computer viruses include antiviral programs, organizational computer-use policies, and federal and state statutes and case law. Each method has strengths and weaknesses. Antiviral programs provide widespread protection but are not foolproof. Establishing well-reasoned computer-use policies can educate many users about preventing the spread of computer viruses, but organizations must be sufficiently well-informed to establish effective policies. Existing computer law prohibits many computer crimes (arguably including viruses), but a prosecutor who wishes to persuade a court to apply general computer law to the spread of computer viruses must understand the technology.

Few legislatures have enacted specific laws to combat computer viruses. As noted above, existing federal law prohibits unauthorized access to federal-interest computers and financial institution computers. Federal law also prohibits intentional access of a federal-interest computer to alter or damage any computer programs or data, if the loss results in damages of over one thousand dollars, or if potential or actual alteration of medical care results. Federal law also prohibits trafficking in computer passwords if the trafficking affects either a federal government computer or interstate commerce. Federal law does not address computer viruses spread in the private sector, however. State laws vary, but may follow a trend toward innovative solutions to combat computer viruses.

Courts have faced an equally challenging task in interpreting traditional laws and specific computer crime statutes. The small body of case law gives little guidance for the new situations that will eventually arise. Of the relatively few computer crime cases prosecuted, many do not appear in case law reporters and none has reached the Supreme Court. Key weaknesses in the computer crime statutes include the failure to define unauthorized access and the inability to determine the value of such intangibles as computer data and use.

Computer virus policy issues include furthering the free exchange of information, determining proper ethical standards, and improving the efficiency of prosecuting those criminals who spread computer viruses. Furthering the free exchange of information should be
balanced against the excessive prohibition of many types of computer conduct. Restrictions that severely impair the free flow of computer information may do more harm than good. The fight against computer viruses is more successful when computer users are encouraged to share information. High ethical standards can help at both the individual and organizational levels. The effectiveness of improved ethical standards may be unlimited, but ethical standards may not be developing quickly enough at present. Prosecution of computer crime lags far behind investigations. Prosecutors must be trained to prosecute computer crimes; victims must more completely disclose computer security failures; and legislative bodies must pass more powerful computer crime laws to fight the spread of computer viruses.

At least three possible federal statutory contexts could aid in the regulation of computer viruses. First, Congress could create a government organization to carry the responsibility and lead the effort to fight computer crime. Such a statutorily created organization (an Interstate Computer Systems Bureau, perhaps) could combine the authority to enforce federal crime regulations with the technical expertise to confront computer crime issues and develop a coherent approach to fighting computer viruses. This bureau could gather accurate, periodic computer crime data; develop policies for prosecution; establish ethical standards; and promote the free flow of information.

The bureau could also support and advise the states, the Congress, and the Executive Branch. Organizations such as the Department of Justice, the Internal Revenue Service, and the Federal Bureau of Investigation could receive information from the bureau and in turn provide helpful service. The bureau could perform a quasi-judicial role in administering rules promulgated under statutory authority granted by Congress, based on the commerce clause of the Constitution. The mechanics of creating such an organization are beyond the scope of this note.

Congress could also take advantage of the FCC's jurisdiction over wire or radio transmission of computer viruses. Because the Communications Act of 1934 gave the FCC jurisdiction over "interstate and foreign commerce in communication by wire and radio,"276 the proposed bureau should focus narrowly on issues within the FCC's jurisdiction, including computer networks using wire or radio transmission. Adopting the FCC standard for carrying

out the bureau’s responsibility would be an action “consistent with the public interest, convenience and necessity.”277 This FCC standard could allow the bureau the flexibility to address changing technologies,278 while preventing an arbitrary or capricious exercise of power. Unfortunately, because many computer viruses are spread by the sharing of programs through means other than wire and radio, an authority based solely upon the FCC could not stop the spread of all computer viruses. For example, one may spread a computer virus simply by allowing a friend to borrow a virus-infected diskette.279

Second, Congress could base computer virus legislation on the malicious mischief chapter of the United States Code.280 One such statute already regulates communication lines.281 The emphasis on intent is appropriate and recognizes a concern for the free exchange of information. Under a malicious mischief statute, lack of intent would excuse a defendant who inadvertently performed an act that caused a criminal result. Again, prohibiting the spread of computer viruses through a malicious mischief statute would require prosecutors to learn to prosecute computer crimes effectively.282

Third, Congress could base computer virus legislation on a theory of fraud.283 A provision for “[f]raud and related activity in connection with computers” already exists.284 Amendment of this section could extend the scope of current computer criminal law while maintaining the coherence and clarity of the law. Still, a “computer fraud” theory for controlling computer viruses has the

---

278. Id.
279. Branscom, supra note 32, at 14–16. A brilliantly designed computer virus, “the Pakistani Brain,” was hidden within program diskettes of such common software applications as Lotus 1-2-3 and Wordstar. Id. George Washington University alone received anywhere from a few hundred to 10,000 reports of the presence of this virus on programs in use. Id.
281. 18 U.S.C. § 1361 (1988). This law applies to “malicious obstruct[ion]” of communication controlled by the federal government. Id.
282. See supra notes 256–70 and accompanying text, which illustrate the necessity for prosecutors to understand computer crime.
same weakness as a "malicious mischief" theory; prosecutors may lack the expertise necessary to enforce the law.

B. Prescription

Because prosecutors lack technical expertise, creating a centralized federal bureau to regulate and protect the free exchange of information within the computer industry would be the most effective way to prosecute the spread of computer viruses. The FCC's Bureau of Common Carriers provides a convenient framework, given the political difficulty of creating another federal agency. The FCC could regulate the spread of computer viruses by wire or radio transmission, which is the means by which the most rapidly spreading, potentially destructive computer viruses are disseminated.

The Federal Communications Act\(^{285}\) establishes the jurisdictional basis\(^{286}\) upon which Congress could protect the free exchange of computerized information and prohibit the spread of computer viruses. Granting the Commissioner of the FCC authority to promulgate regulations for this purpose would assure that the federal agency most experienced at regulating wire transmissions of computerized information has responsibility for regulating computer viruses. Through the FCC and its regulatory authority, Congress could delegate the power to create a flexible system of enforcement by employing knowledgeable computer experts.

Congress could give the Federal Communications Commission authority to regulate the use of computer virus programs by amending the Federal Communications Act as follows: to provide definitions, to authorize a procedure to protect the potential value of computer viruses, to prevent the spread of computer viruses, and to define the penalties for offenders of the statute. Definitions of the terms "knowingly,"\(^{287}\) "recklessly,"\(^{288}\) and "negligently"\(^{289}\) could be taken from the Model Penal Code. The definition of "authorized use" could be borrowed from the New York statute, which provides a means by which computer owners may fairly give notice to a computer user as to the scope of authorized use.\(^{290}\)

\(^{287}\) Model Penal Code § 2.02(b) (1955).
\(^{288}\) Model Penal Code § 2.02(c) (1955).
\(^{289}\) Model Penal Code § 2.02(d) (1955).
\(^{290}\) N.Y. Penal Law § 156.00(b) (McKinney 1988). The text of the provision is cited supra note 89.
The proposed statute would authorize the FCC Commissioner to establish and implement a procedure to allow legal experimentation with computer viruses. Thus, any person with a good reason to use a computer virus for science or education could apply for a permit to execute a computer virus program. The Commissioner would be obliged to pursue the purpose of the statute, which would include the protection of the free exchange of information and the prohibition of computer viruses that are not in the public interest. Because of the highly destructive potential of computer viruses, even persons receiving a computer virus permit would face criminal penalties for the negligent spread of a computer virus.

The proposed statute would prohibit the spread of computer viruses by any means requiring the use of wire or radio transmission. The culpability of an offender would determine the seriousness of the crime. The statute would not use the monetary standard many of the states use because this approach does not consider a defendant's lack of culpability. By penalizing most severely the offenders who best understand the results of their actions, the statute would meet the constitutional requirements of due process and notice. Prosecution would be more effective under the proposed statute than under statutes that include a monetary-based stratification of penalties for offenses.

Under the statute's penalties, a knowing violation would be a felony, a first-time reckless violation would be a misdemeanor, a repeat reckless violation would be a felony, and a negligent violation by a computer virus permit-holder would be a misdemeanor. The maximum fines would correspond to the level of culpability and would increase with repeat offenses. Offenders whose acts constitute felonies could be liable for treble damages, even for a first offense. For the sake of flexibility, the offenses would carry no minimum penalties.

The proposed statute would amend the Federal Communication Act by adding the following new section to Subchapter II, Common Carriers, 47 U.S.C. section 225:

Section 225. Spreading of computer viruses in the District of Columbia or in interstate or foreign communications.

291. Helpful suggestions from Georgia State University College of Law professors Dianne Brinson, Norman Crandell, and Anne Emanuel influenced in part the drafting of the proposed statute. Since the drafting of this proposed statute, H.R. 3524 was introduced in the House. H.R. 3524, 101st Cong., 1st Sess. (1989) [hereinafter H.R. 3524]. H.R. 3524 proposed amending
(a) The purpose of this section is to protect the free exchange of computerized information and to prohibit the spread of computer viruses. The Commissioner may promulgate regulations to enforce this section.

(b) As used in this section-

1. the term "computer virus" means any computer program that copies itself onto or replaces a system start-up program, an operating system program, or an application program.

2. the term "source code" means original computer program instructions.

3. the term "antiviral program" means a computer program that completely ineffectuates the computer virus for which it is designed.

4. the term "knowingly" means the taking of an action with an awareness of the practical certainty of the result of an action.

5. the term "recklessly" means the taking of an action with an awareness of its substantial and unjustifiable risk.

6. the term "negligently" means the taking of an action when there is a substantial and unjustifiable risk of which a reasonable person should have been aware.

7. the term "authorized use" means use of a computer with the permission of the owner of the computer. The computer owner may limit his permission by:

A. giving the user actual notice in writing or orally;

B. posting a written notice in a prominent position adjacent to the computer being used, or

C. using a notice displayed on, printed out on, or announced by the computer being used. Proof that the computer is programmed to display, print, or announce a notice prohibiting copying, reproduction, or duplication shall be presumptive evidence that this notice was displayed, printed, or announced.

the Federal Communications Act to prohibit "the use of interstate communications networks to distribute computer viruses." See 47 U.S.C. §§ 151—609 (1982). H.R. 3524 died in a House subcommittee. The bill did not address the free exchange of information, a serious concern to the Senate Subcommittee on Technology and the Law. Betts, supra note 142. Mr. Betts, after interviewing Senator Patrick J. Leahy, Chairman of the Subcommittee, described Senator Leahy's position as finding computer viruses "criminal and intolerable," but stated that Senator Leahy is "in no rush to pass legislation that might inadvertently stifle experimentation and the free exchange of information over computer networks and bulletin board systems. 'We are probably wise to go slowly and carefully,' [Senator Leahy] said." Id. 292. N.Y. Penal Law § 156.00(6) (McKinney 1988).

293. Id. at § 156.00(6a).

294. Id. at § 156.00(6b).

295. Id. at § 156.00(6c).
the term "computer virus permit" means the Commissioner's certification that a person may cause the execution of a computer virus within that person's authorized use of the virus for scientific or educational purposes.

(c) In granting any computer virus permit, the Commissioner shall have authority to-

(1) require any person requesting a computer virus permit to submit an application which discloses the respective computer virus source code; the source code of the respective antiviral program; the number, location, and identification of any and all computers involved; the names and addresses of the persons the requested permit is to include; and the scientific or educational purposes for spreading the computer virus;

(2) require any applicant to demonstrate the effectiveness of the applicant's antiviral program; and

(3) issue, at the Commissioner's discretion, a permit which may be subject to any other restrictions which the Commissioner may establish to enforce this section in the public interest.

(d) Whoever, in the District of Columbia, in any territory of the United States, or in interstate or foreign commerce, by gift, sale, force, fraud, electronic or radio transmission, or by any other means, causes or attempts to cause a computer virus to come into the possession of another person, or by any means causes or attempts to cause a computer virus to execute in any computer, whether his own or that of another; or

(2) with a computer virus permit-

(A) knowingly, or

(B) recklessly, or

(C) negligently

and contrary to such computer virus permit causes or attempts to cause a computer virus to execute in any computer, whether his own or that of another, shall be punished as provided in subsection (e) of this section.297

296. This subsection of the proposed statute uses some phrases and structure from 47 U.S.C. § 223 (a criminal provision within the Common Carriers Subchapter of the Federal Communications Act).

The punishment for an offense under subsection (d) is:

1. (A) a fine not to exceed treble the value lost as a consequence of the execution of the computer virus in a computer, or imprisonment not to exceed ten years, or both, in the case of a first offense under subparagraph (d)(1)(A) or (d)(2)(A) of this section; and

(B) a fine not to exceed treble the value lost as a consequence of the execution of the computer virus in a computer, or imprisonment not to exceed twenty years, or both, in the case of an offense under subparagraph (d)(1)(A) or (d)(2)(A) of this section which occurs after a conviction for another offense under such subparagraph; and

(A) a fine not to exceed twice the value lost as a consequence of the execution of the computer virus in a computer, or imprisonment not to exceed one year, or both, in the case of a first offense under subparagraph (d)(1)(B) or (d)(2)(B) of this section; and

(B) a fine not to exceed treble the value lost as a consequence of the execution of the computer virus in a computer, or imprisonment not to exceed ten years, or both, in the case of an offense under subparagraph (d)(1)(B) or (d)(2)(B) of this section which occurs after a conviction for another offense under such subparagraph; and

3. (A) a fine not to exceed the value lost as a consequence of the execution of the computer virus in a computer, or imprisonment not to exceed six months, or both, in the case of a first offense under subparagraph (d)(2)(C) of this section; and

(B) a fine not to exceed twice the value lost as a consequence of the execution of the computer virus in a computer, or imprisonment not to exceed one year, or both, in the case of an offense under subparagraph (d)(2)(C) of this section which occurs after a conviction for another offense under such subparagraph.

CONCLUSION: FINDING A CURE

To assure free exchange of information, computer owners must retain the freedom to set their own computer security policies.

296. 18 U.S.C. § 1030(d) (1988). The format and language of this subsection are identical with the exception of the stratification of penalties in the proposed statute, which are based upon whether the violation was committed knowingly, recklessly, or negligently.

299. Id.
Computer owners, including computer security experts, cannot prevent the spread of all types of computer viruses. Further research is needed to reveal methods to permit authorities to prosecute effectively and punish the intentional spread of computer viruses, while promoting the free exchange of information. Such research should include an inquiry into the political and legal requirements for creating a federal agency to regulate the use of computers, including computer viruses. The development of new technology adds both uncertainty and promise to the current development of computer virus law.

Paul Chastain Ray