Incidental Paper

Rogue Computer Programs — Viruses, Worms, Trojan Horses, and Time Bombs: Prank, Prowess, Protection or Prosecution?

Anne W. Branscomb

Program on Information Resources Policy

Harvard University

Center for Information
Policy Research

Cambridge, Massachusetts

An incidental paper of the Program on Information Resources Policy.

Rogue Computer Programs — Viruses, Worms, Trojan Horses, and Time Bombs: Prank, Prowess, Protection or Prosecution?

Anne W. Branscomb

September 1989, I-89-3

Project Director
Anthony G. Oettinger

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Anne W. Branscomb is a communications lawyer and author associated with the Program.

Incidental papers have not undergone the reviewing process the Program requires for formal publication. Nonetheless the Program considers them to merit distribution.

Printing 5 4 3 2 1

September 1989

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Action for Children's Television
American Telephone & Telegraph Co.
Ameritech Publishing
Anderson, Benjamin, Read & Haney, Inc.
Apple Computer, Inc.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Bell Atlantic
Bell Canada
BellSouth Corporation
Boice Dunham Group Inc.
Bull, S.A. (France)
Centel Corporation
Chronicle Broadcasting Company
CMC Limited (India)
Communications Workers of America
Computer & Communications Industry Assoc.
Computer Intelligence
Continental Graphics Corp.
Coopers and Lybrand
Copley Newspapers
Data America Corp.
Data Communications Corp. of Korea
Dialog Information Services, Inc.
Digital Equipment Corp.
Dow Jones & Co., Inc.
Dun & Bradstreet
France Telecom
Gannett Co., Inc.
Gartner Group, Inc.
GTE Corporation
Hitachi Research Institute (Japan)
Honeywell, Inc.
IBM Corp.
Information Gatekeepers, Inc.
Information Industry Association
Interconsult
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
Knowledge Industry Publications, Inc.
Korean Information Society Development
  Institute
Lee Enterprises, Inc.
John and Mary R. Markle Foundation
MCI Telecommunications, Inc.
Mead Data Central
MITRE Corp.
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Corp. (Japan)
Northern Telecom Ltd. (Canada)
Nova Systems Inc.
NYNEX
OTC Limited (Australia)
Pacific Telesis Group
Public Agenda Foundation
Research Institute of Telecommunications and
  Economics (Japan)
RESEAU (Italy)
Rhode Island Public Utilities Commission
Rizzoli Corriere della Sera (Italy)
Saint Phalle International Group
Salomon Brothers
Scaife Family Charitable Trusts
SEAT S.P.A. (Italy)
Southern New England Telecommunications
  Corp.
State of California Public Utilities Commission
State of Minnesota Funding
TEKNIBANK S.p.A. (Italy)
Telecom Australia
Telecommunications Research Action Center
  (TRAC)
Tele/Scope Networks, Inc.
Third Class Mail Association
Times Mirror Co.
United States Government:
  Department of Commerce
    National Telecommunications and
    Information Administration
  Department of Defense
    National Defense University
  Department of Health and Human Services
    National Library of Medicine
  Department of State
    Office of Communications
  Federal Communications Commission
  General Services Administration
  National Aeronautics and Space
    Administration
  National Security Agency
  U.S. General Accounting Office
  United States Postal Rate Commission
United Telecommunications, Inc.
US West
Wolters Kluwer

Acknowledgments

The author wishes to acknowledge the cooperation and assistance of J.J. BloomBecker, Harvie H. Branscomb, Whitfield Diffie, Thomas Guidobono, Leigh Haddon, Donald G. Ingraham, Phyllis Kahn, Daniel J. Kluth, Daniel Knauf, Larry Martin, Davis McCowan, Ronald Palenski, Marc Rasch,[*] Douglas Riggs, and Clifford Stoll.

These individuals and the Program's affiliates are not, however, responsible for or necessarily in agreement with the views expressed herein, nor should they be blamed for any errors of fact or interpretation.

[*] Mr. Rasch did not comment on the Internet Worm.

Executive Summary

- In the late 1980's the computer world has awakened to a new threat to its health -- an infestation of various maladies which collectively, and sometimes erroneously, have been called "computer viruses". ADAPSO, the software trade organization, reported a 10-fold increase in viral infections from 3000 in the first two months of 1988 to 30,000 reported during the last two months of the same year.

- Lawyers, legislators, computer manufacturers, software programmers, and security experts are equally concerned whether or not the people responsible for these various electronic malfunctions can be or should be prosecuted under existing statutes. Several of the most recent incidents include the INTERNET worm, Aldus peace virus, the Pakistani Brain, and the Burleson Revenge. The motives of the perpetrators include pranks, improvement of protection, probative or punitive, prowess, peeping, philosophy, potential sabotage, poverty, and power.

- A range of existing state and federal statutes might cover these sets of facts, and additional bills are pending in Congress and in several state legislatures in the spring of 1989.

- It is difficult to determine strategies since it cannot be ascertained whether the rogue programs are a transient problem which will go away as "hackers" develop a different ethical standard, whether they are a drop in the bucket of problems which may arise as the criminally motivated become more computer literate, or whether they are like the common cold, afflictions which come with the use of computers with which we must learn to live.

Table of Contents

List of Tables

ROGUE COMPUTER PROGRAMS
VIRUSES, WORMS, TROJAN HORSES, AND TIME BOMBS:
PRANK, PROWESS, PROTECTION OR PROSECUTION?

In the late 1980's the computer world has awakened to a new threat to its health -- an infestation of various maladies which collectively, and sometimes erroneously, have been called "computer viruses". A Hebrew University computer scientist has compiled the characteristics of 58 virus strains [87] (see Appendix A), and ADAPSO, the software trade organization, reported a 10-fold increase in viral infections from 3000 in the first two months of 1988 to 30,000 reported during the last two months of the same year. [75]

Lawyers and legislators have become equally concerned whether or not the people responsible for these various electronic malfunctions can be or should be prosecuted under existing statutes. The purpose of this exercise is to review several of the most recent incidents, to review existing state and federal statutes which might cover these sets of facts, and to summarize the bills pending in Congress and considered by several state legislatures in the spring of 1989.

I. RECENT OUTBREAKS OF ROGUE COMPUTER PROGRAMS

A. THE INTERNET WORM

A disease, not unlike the bubonic plague of medieval times, struck the computer world on the evening of Wednesday, November 2, 1988. Of a universe of about 60,000 computers which might have been infected by the strange malady, some 6200 (or about 10%) were slowed down to a halt by what computer specialists call a "worm" and the uninitiated term a "virus" because it spreads rapidly from victim to victim. [see infra, II, for definitions] Injected into the ARPANET, a computer communications system created for academic users by the Defense Advanced Research Projects Agency (DARPA), the "worm" quickly replicated itself into MILNET, an unclassified network of the Department of Defense and INTERNET, which interconnects some 400 local area networks supported by DARPA and the National Science Foundation. [109] Within a few hours, the electronic highways were so congested with traffic that computer specialists around the country went scurrying to their consoles trying to contain it. [75] Indeed, the rogue computer software, or sorcerer's apprentice [105] multiplied so rapidly that efforts of its creator to impede its growth were not effective. [6,74] Eventually major computer centers around the country were involved, including NASA Ames Laboratory, Lawrence Livermore National Laboratory, SRI, MIT, the University of California at both the Berkeley and San Diego campuses, the University of Maryland, Purdue, and the Rand Corporation. It was some 48 hours before calm was restored and the computer networks were back to normal. [41,71,90a]

According to the Computer Virus Industry Association, whose members sell "vaccines" to assist in the rehabilitation of such infestation of computer software, the siege caused an estimated $96 million [19] in labor costs to contain by clearing out the memories of the computers and checking all the software for signs of recovery. Other estimates run as high as $186 million [54]. In the aftermath, more sober minds have calculated that more likely fewer than 2000 computers were affected and the value of the "down time" was closer to $1 million. [105]

According to the experts, no actual damage to the computer hardware or the computer software was inflicted, e.g. no files were destroyed, no software was wrecked, no classified systems were compromised. [111] As a consequence it is not clear that any crime was committed, although a team of investigators went to work immediately to determine whether to indict. It was expected that the INTERNET worm would become the first prosecution under the federal Computer Fraud and Abuse Act. However, there have been two convictions (Mitnick and Zinn) prior to the indictment of the "worm" originator in July 1989. [116] Most computer crime laws require an intent to inflict harm, which was allegedly lacking in this case, [74,109] although some computer scientists purport to identify felonious intent in the subroutines which were encrypted, erased and reconstituted in a manner designed to confuse pursuers on the trail of the intruder. [101]

As the alleged perpetrator was a first year graduate student at Cornell University, there is unlikely any personal source of financial largesse for money damages to be paid under tort law, although his behavior can likely meet the tests of ordinary negligence as well as reckless disregard for the consequences. It is conceivable that some tort action law would lie against Berkeley, where the UNIX program was issued (without charge to other universities) for permitting the imperfections in the software, which facilitated the intrusion, to remain uncorrected. However, many computer programmers found this "trap door" [115] a convenience which did not in any way harm ordinary users. Thus it might be difficult to show that the "trap door" per se was either negligent or the proximate cause of the harm which occurred. It is also possible that a suit in tort might lie against one of the universities for failure to exert due supervision over its authorized users, although Cornell has completed an extensive investigation purported to exonerate it from any actionable negligence. [71] The National Center for Computer Crime Data has reported no damage suits filed against computer network or service providers. [27]

Certainly the methodology was clandestine. According to friends, the student entered the virus remotely via a computer at MIT. [56] The program code was encrypted and designed to assume the identity of other users and report back to a remote computer suggesting an audit trail that would lead to other points of entry as the source of the questionable code. [101]

Ironically, the alleged culprit (who reportedly danced on the desk top when he discovered the "trap door" in the Berkeley version of UNIX through which he could insert his computer program) [74] is a bright young 23 year old graduate of Harvard University where he was so trusted that he was given "super user" status on the Aiken Computers in order to assist in their maintenance. [56,111] Friends reported that his motives were to test the vulnerability of the system in order to learn how to make it more secure. [48]

Young Robert T. Morris, Jr., or RTM, as he is known for his computer "log-on" ID, is the son of the chief scientist of the National Computer Security Center, a nationally recognized and highly respected expert on computer break-ins, a 26-year veteran of the Bell Telephone Laboratories, and (not entirely coincidentally) one of the three designers of the first known computer virus played as a high tech recreational game (CORE WAR) by computer programmers after hours to hone their skills. [41] Indeed, Robert T. Morris, Sr., testified before

Congress several years ago, in an inquiry into the effects of computer viruses, that it would be a good omen if young computer scientists were so skilled as to be able to write such sophisticated programs:

> The notion that we are raising a generation of children so technically sophisticated that they can outwit the best efforts of the security specialists of America's largest corporations and or the military is utter nonsense. I wish it were true. That would bode well for the technological future of the country. [111]

Thus the nature of the incident and the identity of the initiator suggest a dilemma as to whether or not criminal punishment is appropriate under the circumstances. Many computer scientists have been reported to predict that the younger RTM will mature and "make important discoveries in the computer field". [93] Indeed, among some of the young computer literati (often referred to as "hackers"), RTM is looked upon as a folk hero. [90] Even among the more seasoned citizenry, many equate RTM's behavior with that of Matthias Rust, the young German, who flew his small plane through the Soviet border controls and landed in Red Square. [48] Some even laud the invasion of the INTERNET worm as precipitating a therapeutic look at the security of the systems, because the incident has sent multitudes of computer professionals to the drawing boards to design more impenetrable network environments. [38,56,73,111]

However, a more secure system may be a deterrent to the flexibility and openness which have characterized the UNIX operating system, originated by AT&T and designed to encourage the open network access which facilitates intercourse among multiple users.

Federal officials were, according to published reports, at odds on the nature of the indictment. The U.S. Attorney for the Northern District of New York (where the entry point to the network originated at Cornell) [71] was reported to favor plea bargaining a misdemeanor conviction in exchange for further disclosure of the circumstances surrounding the incident, whereas the Department of Justice lawyers and the Federal Bureau of Investigation reportedly favored felony charges as a deterrent to would be computer hackers, telephone "phreakers" and other assorted pranksters. [1,90]

On the other hand, if criminal laws are not the answer, and tort laws not efficacious, what sanctions are appropriate to deal with reckless drivers on the electronic highways of the future?

B. THE ALDUS PEACE VIRUS

On March 2, 1988, the anniversary of the advent of Apple Computer's MacIntosh II and SE models, the following message popped up on the monitors of thousands of MacIntosh personal computers in the United States and Canada:

> Richard Brandow, the publisher of MacMag, and its entire staff would like to take this opportunity to convey their universal message of peace to all MacIntosh users around the world. [106]

Beneath the message appeared a picture of the globe. Brandow, publisher of a computer magazine based in Montreal, Canada, acknowledged in a telephone interview to an Associated Press writer that he had written the message. However, he only intended to show how widespread software piracy had become and expected the "virus" to make its way around a limited perimeter centered on the Montreal area where he had made disks available containing the message in question. The message had been conceived some year or so earlier and previously tested by its designers -- a co-worker, Pierre M. Zovile, and Drew Davidson of Tucson. [41,53,57,106] According to Brandow, it was imbedded in a popular game program called "Mr. Potato Head" and left on a MacIntosh in the offices of MacMag, a popular gathering place for MacIntosh users, for only two days during a Mac users conference. [106]

The message later turned up in Freehand, a program distributed by the Aldus Corporation, a software company based in Seattle, Washington, precipitating the recall of some 5000 copies of the program. [106] This is the first known contamination of off-the-shelf (commercially marketed) software, since it had been assumed in the past that such viruses were distributed in freely exchanged disks or on electronic bulletin boards. [63] The transfer to commercially marketed software was accomplished, without his knowledge, by Marc Canter, President of Macromind, Inc., of Chicago, Illinois, who reviewed the infected disk on a computer which was later used for copying of a self instructional program intended for distribution by the Aldus Corporation. Less than half of the duplicated disks were actually distributed to retailers, but the computer industry has become permeated by fear of viral contamination, as many of the major software companies are customers of Macromind, including Ashton-Tate, Lotus, and Microsoft. [63]

Canter claims that Brandow gave him the disk, but Brandow denies doing so, although he admits meeting Canter. Lotus, Microsoft, and Apple claim that none of their products has been contaminated, and Ashton-Tate has declined to comment. However, Apple hastened to design and give away for free on many electronic bulletin boards and networks, a vaccine which would remove hidden code in tainted programs. [106]

According to the best available information, the program was "benign" in that it destroyed no files, interfered with no functions, and erased itself after popping up on the computer screens as triggered by its timing device on March 2, 1988. [57,63]

C. THE PAKISTANI BRAIN

In the late spring of 1988, Froma Joselow, a reporter for the *Providence Journal Bulletin*, of Providence, Rhode Island, booted a disk containing the last six months of her work product including the notes for the article she intended to write. After writing the article, she entered "PRINT", but the screen came up blank then displayed the following "advertising message" on her computer monitor [41]:

```
WELCOME TO THE DUNGEON
©1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
[address and telephone in Lahore, Pakistan]
Beware of this Virus
Contact Us for Vaccination [59]
```

This was a well-designed and cleverly executed device by two Pakistani brothers, Amjad Farooq Alvi (age 26) and Basit Farooq (age 19), who studied physics at Punjab University, taught themselves computer programming, and operated a small computer store in Lahore, Pakistan. According to an interview given to a reporter for *The Chronicle of Education*, Basit admitted introducing the message, which was well hidden within popular software, such as Lotus 1-2-3 and Wordstar, "for fun". [59] He disavowed any knowledge of how it came to reside in the computers of the *Providence Journal Bulletin* or on the disks of hundreds of students at the Universities of Pittsburgh, Pennsylvania, Delaware, George Washington, and Georgetown. [53]

Later Amjad admitted that their original intentions had been to protect their own computer software from local pirates who would have to contact them to decontaminate the disks which had been copied rather than purchased. [53] As the program evolved, however, it was deliberately imbedded in commercially available and copyrighted software which the Farooq brothers sold to foreigners, especially Americans. "Because you are pirating, you must be punished", Amjad was quoted as saying, thus admitting to be an accessory to a form of electronic lynching in order to punish foreigners who were contravening their own law while Amjad was selling uninfected disks to his own countrymen. Computer software was not then covered by Pakistani copyright statutes, so it was quite legal, under Pakistani law, to import from abroad expensive issues of computer software and resell copies on the domestic Pakistani market for as little as $1.50. [41]

According to Harold Highland, editor of *Computers and Security*, the Pakistani Brain virus was very sophisticated and cleverly designed. [59] It never infected a hard disk and was quite media specific, imbedding itself only into DOS formatted disks. One admirer complimented Amjad, "This virus is very elegant. He may be the best virus designer the world has ever seen." [41]

However, this brotherly calling card was quite destructive, attacking the disks primarily of university students and journalists. It was less troublesome systemically, because it did not attack hard disks or main frames or enter any widely used computer networks. However, at least one PhD thesis was destroyed, and various versions continue to erupt in one part of the world or another. For example, a second infestation of the Pakistani Brain virus erupted in November 1988 in the School of Business at the University of Houston, this time in a slightly modified version but with the old copyright notice! [56]

It is difficult to ascertain how many users were affected, as the reports vary from a few hundred to more than 100,000 IBM PC disks with an estimated 10,000 at George Washington University alone. [41]

D. THE BURLESON REVENGE

On September 21, 1985, an employee of the USPA & IRS, Inc, a brokerage house and insurance company in Fort Worth, Texas, discovered to his dismay that 168,000 of the firm's sales commission records had vanished without a trace. The only clue was an unusual entry into the computer at 3:00 a.m. earlier that morning, a time when no employee should have been operating the system. Working all weekend, the MIS crew restored the records from backup tapes, thinking they had repaired the damage. On the contrary, when other employees reported for work on Monday morning and turned on their computer consoles, the entire system "crashed" and became inoperable. Reconstructing the pathway to this crisis, the audit trail led to an instruction "power down" which was invoked by a simple retrieval command. The computer professionals referred to the intricately designed software as "trip wires and time bombs" designed "to wipe out two sections of memory at random, then duplicate itself, change its own name, and execute automatically one month later unless the memory area was reset." [64] No permanent damage was done to the system and the MIS staff were able to reconstruct the system from scratch including installing a new operating system from IBM. [79]

The breach of security was eventually determined to be the work of an employee, with access to all of the passwords of the company, who had been dismissed three days earlier. Donald Gene Burleson, who was variously described as arrogant, rebellious against authority, and a superbly skilled programmer, was ultimately indicted and convicted of computer abuse under the Texas Penal Code [SS. 33.01-.05] which permits a felony charge to be filed if the damage exceeds $2500 from altering, damaging, destroying data, causing a computer to malfunction or interrupting normal operations. Moreover, the Texas statutes provide for a misdemeanor of using a computer or accessing data without the consent of the owner. Burleson was likely guilty of all of the above.

There was no question that there was "malice aforethought" as the "power down" function had a creation date of September 3, almost three weeks before the execution. Burleson's dismissal came not from any lack of skill in the execution of his normal duties; it came from his "misuse" of the company's computers to aid and abet in his philosophical and fanatical opposition to the income tax in his support of the now jailed Irwin Schiff, who propounded its unconstitutionality. [49]

E. OTHER WELL-KNOWN VIRAL INFECTIONS

One of the earliest virus outbreaks, which was treated as a hacker's prank, was the program known as "The Cookie Monster". When serious students were busy at their consoles a message would pop up on the screen "I want a cookie!". The message would not go away, thus disabling further work, until the weary student figured out that it was necessary to enter "COOKIE" on the keyboard. [58] In a similar vein is the PAC MAN program, considered by some to be a "delightful hack", which devours the file on the screen and the PING PONG (or Italian) virus which bounces ping pong balls across the screen. [36] Other more deleterious programs devoured all memory then gloated on the screen with a message which said "Arf, arf, Gotcha!" [41]

Most of the earlier "virus" programs were characterized as more or less harmless computer games. These replicated in the electronic environment the not always benign tricks or pranks which college students play on each other. A more devastating prank was a program listed as RCK.VIDEO with an animation featuring the popular singer Madonna which erased all files while she was performing then announced to the bewildered viewer, "You're stupid to download a video about rock stars." [41]

Not quite so benign in its consequences either was the IBM Christmas card which was innocently sent to a friend by a West German Law student through the European Academic Research Network (EARN) in early December of 1987. [85] The message, with a Christmas tree graphic, was sent through an electronic mail system designed to resend itself to all addresses on the addressees' mailing lists. [76] So promptly did this message propagate itself that the entire internal IBM messaging system, which reaches 145 countries, was brought to a halt by the runaway Christmas spirit. [53] IBM only acknowledged to its employees on December 14, 1987, that a "disruptive file" entitled "CHRISTMA.EXEC" had produced "an excessive volume of network traffic" and was an inappropriate use of IBM assets. [4]

The "viruses" described above had no special capability to violate security except by discovering and copying names and addresses, passwords, or ID's. Thus it is assumed that no high level secured computers have been compromised by destructive rogue programs. However, much publicity has circulated concerning the antics of members of a computer club in Hamburg, West Germany, called CHAOS, whose presence has been perceived in numerous high level government computers in Europe and the United States. [76] According to Herwart "Wau" Holland (age 36), the club's founder, the entire purpose of the club is creative and benevolent -- e.g. to increase the flow of public information which is tightly held and controlled by overly zealous public authorities. [96] Indeed, the group were said to be quite instrumental in keeping the press well-informed concerning the Chernobyl incident, contradicting official reports designed to calm the fears of the population. [53]

Systems managers who have diligently observed the persevering and plodding efforts to crack open the closed computer networks are not so kind in their characterizations of these electronic "break-ins", since it is impossible to tell the difference between voyeurism and espionage. [105] Also unimpressed are security officers of the systems who find that their protective protocols have been penetrated when they discover the "calling cards" left by CHAOS members. So far these have been benign and seem to fall in the category of the "Kilroy was Here" graffiti which adorned many edifices during World War II. The primary vice other than "unauthorized entry" would appear to be publicizing the methods used for "breaking and entering". [28]

Not everyone condemns the activities of the CHAOS Computer Club. Some observers applaud the efforts of these electronic Robin Hoods to disseminate the riches of the information age to the information poor. [70,96,102] As for CHAOS, its leaders disavow any purpose other than to expose excessive government secrecy to a little therapeutic sunlight.

Most of the highly sensitive national security and financial industry systems have either not been breached or those who have suffered viral maladies are not admitting to any harm. However, a number of intracorporate networks have been invaded, and recently the Databank System, Ltd., in Wellington, New Zealand, was the first electronic funds transfer system to admit publicly that it had been infected with a virus which read "Your PC is Now Stoned! LEGALIZE MARIJUANA!" [56]

On Friday, January 13, 1989, hundreds of commercial and home computers in the United Kingdom reported what was assumed to be a reappearance of the virus which had been identified in Israel at the Hebrew University before it sprang to life on a previous Friday, May 13, 1988. [2,51] A similar "Friday, the thirteenth, virus" invaded the international network of the Digital Equipment Corporation (DEC) in January of 1989. [90]

The Soviet Union has not escaped infection, as Sergei Abramov, a computer specialist at the USSR Academy of Sciences revealed on Radio Moscow in December 1988. A group of Soviet and foreign school children attending a summer computer camp unleashed the "DOS-62" virus which affected 80 computers at the academy. Prior to August of 1988, there had been no evidence of such infestations, but since then two distinct viruses have turned up in at least five different locations. [82]

Clearly, the virus epidemic is a global problem which cannot be contained merely by state or even national laws but will likely require a considerable amount of coordination at the international level if the electronic highways are to be safe. However, the problem of containment cannot be any more challenging than controlling the highwaymen of medieval times or the pirates of the high seas.

II. TYPES OF AFFLICTIONS

In order to understand better the analysis of current laws and their efficacy it is useful to distinguish between the terms used to apply to various outbreaks of electronic maladies. These are summarized in Table 1.

Table 1

Case Studies: Types of Rogue Programs

	TYPE OF ROGUE PROGRAM			
	VIRUS	WORM	TROJAN HORSE	TIME BOMB
	Name of Rogue			
	Pakistani Brain	RTM's Great "Hack"	Aldus Peace Message	Burleson's Revenge
Benign		✓	✓	
Malicious	✓			✓
Protective	✓			
Disruptive		✓		
Destructive	✓			✓
Costly		✓		✓
Punitive	✓			
Prowess		✓	✓	
Revengeful				✓
Instructive			✓	
Prankish			✓	

A. VIRUS -- according to most computer experts, a virus is, like its namesake, a carrier of electronic messages which not only invades other programs but is designed to modify the invaded hosts and to replicate itself. The prosecutors in the Burleson case in Fort Worth, Texas, did not characterize that situation (deliberate destruction of data within the company's mainframe computer) as a virus. However, the expert witness for the defendant did so characterize the program, because it was so designed that it deleted itself once it had finished its monthly rampage. It then erased its trail but not without replicating its destructive capability in another set of programs with a different sequence of names which remained present to become active the following month.

B. WORMS -- take up residence as a separate program in memory thus proliferating and using up storage space which may slow down the performance of the invaded computers and/or bring them to a halt. According to researchers at the Xerox Palo Alto Research Center a worm is "simply a computation which lives on one or more machines" segments of which remain in communication with each other [97a].

C. TROJAN HORSE -- a desirable program which contains a parasite or viral infection within its logic which is undetectable upon casual review.

D. TIME BOMB (OR "LOGIC BOMB") -- an infection intended to launch its attack at a preset time. The Aldus virus was a "time bomb" triggered to display its message on March 2, 1988, whereas the Hebrew University "time bomb" was triggered to go off on every Friday 13th, and the Burleson "time bomb" was designed to destroy the company's files monthly.

III. MOTIVATIONS OF THE INTRUDERS

An analysis of the purposes for which these rogue programs are written discloses the following, as listed in Table 2:

A. PRANKS -- These would appear to be overwhelmingly the most numerous and, in most cases, benign.

B. PROTECTION -- In many cases, the motivation seems to have been an exercise in understanding how to penetrate systems in order better to protect them. Indeed, such penetration of security systems has demonstrated skills which have led some of the "hackers" into employment as security consultants. Now that the authorities are cracking down on unauthorized entry and use of computer resources, some of the new breed of "hackers" express genuine consternation at the change in expectations.

Table 2

Motivations of Intruders

Motivations	
A.	Pranks
B.	Protection
C.	Punitive
D.	Prowess
E.	Peeping
F.	Philosophy
G.	Potential sabotage
H.	Poverty
I.	Power

C. PROBATIVE AND/OR PUNITIVE -- In some cases the purpose has been a self-described posse, as in the case of the Farooq brothers. They originally sought a way to track piracy by forcing the software pirates back into their computer shop to charge them for stealing product which the local law did not protect and ended up imbedding their own deadly poison to punish foreign customers for what they perceived to be unethical purchases of their own countrymen's product.

D. PROWESS -- Much of the unauthorized entry would appear to be accomplished by young computer enthusiasts seeking thrills by exercising their computer skills. This appears to be by far the most prevalent motivation among the so-called "hackers" such as RTM, many of whose young admirers thought he had achieved the "ultimate hack". Indeed, the original use of the word was to describe programmers who were capable of writing elegant code which was the envy of their colleagues. In this respect the "hackers" are not unlike the "hot rodders" of the 1930's who souped up the engines of Model T Fords and learned mechanical skills to which was attributed much of the success of the technical support in World War II. [38]

Most "hackers" become responsible professionals as they grow older, leave protected and subsidized academic computer networks, and have to earn their own way in the world. However, some of these apprentices have turned their skills to damaging and socially unacceptable behavior. Indeed, the lawyer for Kevin David Mitnick (well known in the computer world by his moniker "Condor" and convicted in early 1989 under the federal computer fraud act), described his miscreant behavior as efforts to achieve self esteem, "an intellectual exercise ... [to] see if he could get in. It's Mt. Everest -- because it's there." [83] The director of the Computer Learning Center in Los Angeles, where he was a student, described his skills as quite outstanding. [89] "Hackers", such as Mitnick, can be characterized as "technopaths", a term coined by A.K. Dewdney. [75]

E. PEEPING -- This would appear to constitute a sort of electronic voyeurism. Such unauthorized entries would not qualify as "viruses" unless the voyeur left a "calling card" which contained a self-replicating message.

F. PHILOSOPHY -- Many of the computer "hackers" look upon information as a public good which should not be hoarded; therefore, entry should not be prohibited. They can be characterized as "Information Socialists" who believe that all systems should have open access and their contexts be shared. This view is best expressed by Richard Stallman of MIT's artificial intelligence laboratory, a dedicated lobbyist for this point of view. [102] He claims that the aberrant ones are those who try to fence off information systems and stake out property rights in what should be, like the high seas and outer space, "the common heritage" or "the province of mankind".

G. POTENTIAL SABOTAGE -- There has, as yet, been revealed to the public little evidence of the work product of terrorists invading computer systems, although there have been reports that both the Central Intelligence Agency (CIA) and the National Security Agency (NSA) are experimenting with the use of viruses as a strategic weapon. [86] The Pentagon announced in early December 1988 that it had established a SWAT team to combat invasive programs such as the INTERNET worm. [12a,17] Administered by the Computer Emergency Response Team Coordination Center, the team is on 24-hour alert. [75]

There is evidence that some of the systems purported to be the most secure in design have been penetrated by voyeurs if not by viruses. The young accomplice of Mitnick who turned him in to the authorities was quoted as saying, "Our favorite was the National Security Agency computer because it was supposed to be so confidential. It was like a big playground once you got into it." [3a] Mitnick, who was well known to law enforcement officers around the country, was called by them "an electronic terrorist" who was addicted to breaking into secure computer systems. [62] Ironically or perhaps justifiably, the last caper (among many for which he was convicted) was theft of a new program designed by Digital Equipment Corporation to help users identify such unwanted invaders as Mitnick himself. [15]

Many computer scientists and government officials fear that the pranksters and computer professionals who manipulate the software "for fun" or "for fame" may instruct potential saboteurs and terrorists on how to achieve their more destructive purposes. Thus there was a substantial disagreement among computer scientists over the request by the National Computer Security Center (NSSC) for Purdue to keep secret the details of the INTERNET worm's source code, which they decompiled. [13] Many managers of information systems are opposed to such secrecy, because they want to know the internal structure of the offending code in order to better protect their computers from further attack of viral infections.

Thus one question for legislators and educators is how to provide a challenging electronic playground in which young apprentice programmers can cut their teeth without wreaking havoc on the nation's privileged and/or proprietary strategic, financial, and commercial networks.

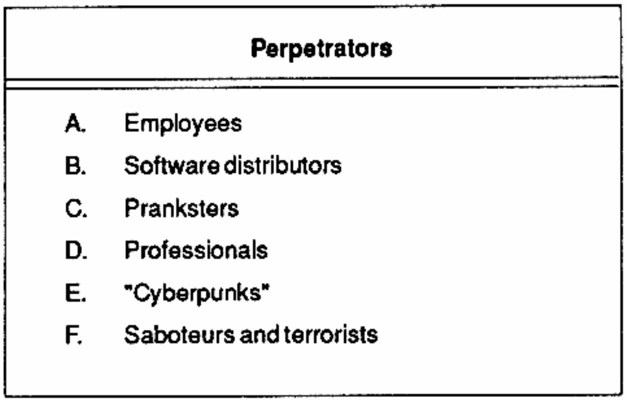
H. POVERTY -- Many of the perpetrators in the electronic environment, as in the physical environment, simply want something they don't have and use whatever means are available to them to acquire what they desire.

I. POWER -- Some unauthorized entry is motivated merely by a desire to exert control over the environment in which the entrant has some skills which are superior to others operating in the same environment. They can be characterized as the "bullies" of the playground. The difference is that their playground is an electronically mediated rather than a physically contained "playground".

IV. PERPETRATORS

Table 3

Types of Perpetrators of Rogue Programs



Perpetrators

A. Employees
B. Software distributors
C. Pranksters
D. Professionals
E. "Cyberpunks"
F. Saboteurs and terrorists

From a review of the above cases, it would appear that a there are a variety of perpetrators, some of whom can easily be characterized as maliciously motivated but many of whom cannot. These include the following, summarized in Table 3:

A. EMPLOYEES -- Most of the devastating incidents are caused by authorized employees acting outside the scope of their employment for their own benefit or to the detriment of the organization. Certainly this was the case with Donald Gene Burleson, the first person convicted under a state law for behavior characterized by his own expert witness as inserting a computer virus. The number of such incidents is unknown, since it is thought to be information tightly held by the companies afflicted. Indeed, in one known case the employee was dismissed quietly but given a lavish going away party to disguise the nature of his exodus from the company. [53]

B. SOFTWARE DEVELOPERS -- Developers of software initially turned to protected disks which performed not at all or badly when copied without authorization. These contained "bugs" or malfunctions deliberately written into the software code in order to prevent piracy. This was the case with the Pakistani Brain Virus. There is likely to be less of this type of situation as the major software firms discovered that sales were inhibited by substantial user abhorrence of this technique.

However, it is well known that some software programs have imbedded, within their code, logic sequences designed to disable use of the programs at the termination of a lease. Thus laws designed to reach secret messages entered without notifying the user might overreach their intended purpose and catch in their net practices considered by the industry as both efficacious and desirable.

C. PRANKSTERS -- The word pranksters is used more aptly than "hackers" to describe young computer users, mostly in their teens, attempting to develop their computer skills and deliberately, but usually not maliciously, entering systems purportedly closed to them. Damage, when it occurs, is usually characterized by ineptness rather than intent, since their intent is merely to "beat the system" to prove how clever they are. This type of incident is characterized by the so-called "Milwaukee Microkids" who ran rampant through many of the major computer systems of the U.S. government and played havoc with the monitoring systems of cancer patients in a New York city hospital in 1983. The FBI took concerted and coordinated action against the "microkids", seizing the computers of a number of these youngsters, in order to send a message of disapproval to all potential pranksters. [11]

D. PROFESSIONALS -- In this category should be included the so-called "hackers", a term which originally applied only to skilled computer programmers who genuinely felt that computer systems should be open. Such "hackers" believed the effort to improve computer software was an ongoing process in which all the "cognoscenti" should be able to participate, and they were committed to designing advanced computer hardware and software. [70] The Cornell report carefully avoids using the word "hacker" pejoratively. [71]

Because of the detrimental consequences of some of the "hacking", the term has been used in the press to mean skilled computer professionals or students with an intent to perpetrate an antisocial act of theft, embezzlement, or destruction. Thus "professionals" fall into three categories: those with criminal intent, those who are apprentices attempting to improve their skills, and those who are deliberately attempting to break into closed systems in order to test their vulnerability and increase awareness of the defects. The latter case is much like the antic efforts of Nobel laureate physicist, Richard Feynman, at Los Alamos, who broke into the safes of his colleagues leaving only an amusing "calling card" to prove his successful entry, thereby proving that they were quite vulnerable to spies. [44a, 45] So-called "tiger teams" have been organized by several government agencies to provide a similar service to stimulate better security measures. [86]

E. "CYBERPUNKS" -- This is a term which has come to be used in describing computer-skilled but anti-social individuals who deliberately disrupt computer systems merely for the joy and personal satisfaction which comes from such achievement. The term is derived from a popular science fiction genre which describes such "cyberpunks" as engaged in sophisticated high technology games. They constitute a form of outlaw society akin to the gangs or teenagers who roam the poverty-stricken areas of inner cities, where young people have nothing better to do to satisfy their egos than take control over their areas of habitation. To some extent the "cyberpunks" are motivated also by a desire to take control over their electronic environment.

F. SABOTEURS OR TERRORISTS -- So far there have been no publicly disclosed incidents of entries resulting in deliberate destruction or interruption of service attributed to terrorists groups, although there have been incidents of espionage. However, there is much apprehension among computer security officials that terrorists are capable of acquiring sophisticated computer programming skills and may apply them to the many networks upon which international commerce, finance, and industry have come to rely. [53a]

V. COVERAGE OF STATE STATUTES

Although only one of the 50 states (Vermont) does not have some kind of computer crime or computer abuse law, the Burleson case is the first conviction under one of them for inserting into a computerized environment what has been characterized by some (but not by others) as a computer virus. Thus its implications have created much interest among law enforcement officers and computer professionals concerning this new threat to computer integrity. Unfortunately, the case does not offer much insight into the applicability of other state laws to computer virus cases. It was a rather clean cut fact situation in which the perpetrator was a disgruntled employee who had been dismissed but retained access to the security codes of the company. His retaliation was easily proved to be maliciously inspired. Moreover, the prosecution was conducted by a young prosecutor who was skilled and understood the nature of the behavior which was offered in evidence in the trial. However, the brightest spot in retrospect is that the jury disclaimed any difficulty in following the case or in reaching its conclusions. [79]

The long delay of the prosecutors deliberating whether to indict RTM in the INTERNET worm case demonstrates the difficulty in proving beyond a reasonable doubt that criminal behavior has occurred without an admission on the part of the perpetrator that such was his or her intent. [56,71] In this case, the audit trail would uncover that the point of entry of the virus into the system was an MIT source and that the program code required the virus to report back to a Berkeley node whenever it succeeded in invading another host. Thus, without the surrounding circumstances of a telephone call to a friend in the Aiken Laboratory at Harvard University warning that "his virus had kind of gotten loose", [109] and the software designer's error in the code which never reported back to the Berkeley computer, an intended saboteur might easily have caused the disruption within the nation's academic networks without leaving a trace of the actual origin.

It can be concluded, from a review of state laws, that they cover a variety of circumstances and fall into several different categories. The Burleson case might have easily been prosecuted under the majority of state laws, because files were destroyed and most of the state laws use the words "alter, damage, or destroy". However, it is not so clear that the INTERNET worm situation falls within the ambit of more than a few of the state statutes, since the damage which resulted was loss of memory and inability of the computer networks to accommodate their users in the manner to which they had become accustomed to expect.

The state statutes cover at least 11 distinct categories of offenses which will be discussed sequentially. They are as follows:

-- those in which the current criminal statutes have been modified to include information residing on a computer disk or within a computer network or mainframe within the definition of "property",

-- those in which the acts to be prohibited clearly cover altering, damaging, or destroying a computer program or files,

-- those in which a computer or its capacities are used to aid or abet the commission of any other crime, e.g. theft, embezzlement, or fraud,

-- those which treat the antisocial acts as "crimes against intellectual property",

-- those which include mere "knowingly unauthorized use" of a computer or computer service as unsanctioned behavior,

-- those in which merely unauthorized "copying" of computer files or software is prohibited,

-- those which cover behavior which disables access or denies the use of the computer to authorized users (which appears to be the situation in the case of the INTERNET worm),

-- those which prohibit the unauthorized addition of material into a computerized environment, which appear to be broad enough to cover the Aldus virus, the behavior of which was quite benign,

-- those which prohibit mere "peeping Toms" e.g. where the unauthorized use is only the time expended in viewing files,

-- those which prohibit "taking possession of" a computer program, and

-- those which provide for compensatory or punitive damages emanating from the prohibited behavior.

A. DEFINITION OF PROPERTY EXPANDED

Typical of the first type are the Massachusetts and Montana statutes. Montana merely defines "property" as including "electronic impulses, electronically processed or produced data or information, ...computer software or computer programs, in either machine- or human-readable form, computer services, any other tangible or intangible item of value relating to a computer, computer system, or computer network, and any copies thereof." [S. 45-2-101(54)(k)]. The Massachusetts statute [chapter 266 S.30(2)] is even more succinct, defining "property" as including "electronically processed or stored data, either tangible or intangible, data while in transit...".

Although the statutes define property as including computer-mediated information, this does not necessarily resolve the problem of a conviction under larceny or theft. Usually the requirement for a conviction is a "taking" with the intent to deprive the owner of the possession or use thereof. Voyeurism with no intent to deprive or harm and/or viruses which have benign consequences, such as the Aldus virus, do not deprive the owner or user of access to or use of any computer files or computer services, except perhaps momentarily while an unwanted message appears on the screen. In the United States, however, unwanted messages are tolerated in many media, e.g. direct mail and television. Thus it must be the apprehension of harm which is the objectionable consequence. Costs are incurred to verify that no damage has been done, and recent legislative efforts are beginning to address this problem. [e.g. Oklahoma, S.1096, Sec.4-C]

B. UNLAWFUL DESTRUCTION

Many of the state statutes contain the legal words of art "alter, damage, delete, destroy". This would appear to be the most common form of computer abuse statute and sufficient to cover the most dangerous forms of activities. Presumably viral code requires some alteration of the sequences in the computer memory in order to function, but it appears that a worm can be inserted by an authorized user without altering any existing files or the operating system.

On the other hand, the Illinois statute [S.16D-3 and 4] seems to be written more broadly, referring to the crime of "computer tampering". However, this offense includes more particularly disruption of vital services of the state, as well as death or bodily harm resulting from the tampering. This would presumably include modification of medical records which were the proximate cause of death or resulted in the negligent treatment of patients.

C. USE TO COMMIT, AID, OR ABET COMMISSION OF A CRIME

Most of the state laws clearly cover use of a computer to commit a crime. Typical of this is the Arizona statute [S. 13-2316] which penalizes the use or alteration of computer programs with the intent to "devise or execute any scheme or artifice to defraud or deceive, or control property or services".

D. CRIMES AGAINST INTELLECTUAL PROPERTY

The Mississippi statutes [S. 97-45-9] provide for a specific prohibition of "offenses against intellectual property" defined as:

> (a) Destruction, insertion or modification, without consent, of intellectual property, or
> (b) Disclosure, use, copying, taking or accessing, without consent, of intellectual property

Although the act requires that such acts be intentional and not accidental, it does not require that they be malicious or harmful. Thus the most innocent voyeurism, even though no actual damage occurred, could be "accessing" within the meaning of the act. Nonetheless, the magnitude of the penalty is related to the malice or harm.

E. KNOWING UNAUTHORIZED USE

The Nevada statute [S.205.4765] is typical of this group of statutes which broadly define "unlawful use" to include "modifies, destroys, discloses, uses, takes, copies, enters", although this does not specifically include the prevention of authorized use by others as in the case of the INTERNET worm. However, the Nebraska statute [28-1347], which contains the phrase "knowingly exceeds the limits of authorization", would likely cover the RTM behavior if it were proved to be as is currently reported.

The Ohio statute prohibits the "unauthorized use of property" [S. 2913.04] which is defined to include "computer data or software" [S. 2901.(J) (1)] and has what appears to be the broadest prohibition of "...any use beyond the scope of the express or implied consent of, the owner..." [S.2913.04 (D)]. The New Hampshire statute [IV (a)] refers to "causes to be made an unauthorized display, use or copy in any form". These two statutes are surely broad enough to encompass the Aldus virus, which was benign yet disturbing, because users were not assured that it was benign when it popped up on their screens.

F. UNAUTHORIZED COPYING

The New York statute prevents both unauthorized duplication [S.156.30] as well as receipt of goods reproduced or duplicated in violation of the Act. [S.156.35] Very few of the states have included provisions of this type.

G. PREVENTION OF AUTHORIZED USE

About a fourth of the states refer to interfering with or preventing normal use by authorized parties. This presumably would cover the existence of a worm, such as the INTERNET worm, which allegedly did no actual damage to files, software, or equipment but occupied so much space in memory that it exhausted the computers' capacities and prevented normal functioning of the networks. Typical of this type of statute is the Wyoming statute [S.6-3-504] which describes "crimes against computer users" as either "knowingly and without authorization" accessing computer files or denial of services to an authorized user.

H. UNLAWFUL INSERTION

The Connecticut statute, which is probably the most comprehensive of the state laws, provides for "intentionally makes or causes to be made an unauthorized display, use, or copy in any form of data..." [S. 53a-251 (e)]. The Delaware statute also refers to interrupting or adding data [S.935 (2) (b)] and the Mississippi statute includes "insertion" of material without authorization as a specifically prohibited act [S.97-45- 9]. It would appear that no harm need occur for these offenses to be committed, although the Delaware statute does key the penalty to the amount of harm resulting. Moreover, a prosecutor may fail to prosecute if the penalty does not seem to fit the nature of the crime. Thus overreaching statutes may not be objectionable, if they are rationally administered. However, the risk is incurred that an overzealous prosecutor might jail a bunch of gifted pranksters, thus jeopardizing the development of a computer-skilled work force.

I. VOYEURISM

A few of the statutes cover unauthorized entry for the purpose only of seeing what is there. Thus the Missouri statute [S.569.095 (5)] refers to "intentionally examines information about another person" as a misdemeanor, thus recognizing a right of electronic privacy. On the other hand, the Kentucky statute [S.434.845] specifically excludes from criminal behavior accessing a computerized environment "only to obtain information and not to commit any other act proscribed by this section"; thus mere voyeurism is excluded from prosecution.

J. "TAKING POSSESSION OF"

Several of the statutes refer to taking possession of the computer. It is not clear whether or not this term is intended to cover the kind of anti-social behavior described above as that of "cyberpunks", although actual theft of the computer itself would surely be covered under the normal definition of theft of physical property, so it must be assumed that some other meaning was intended by the drafters. The Wisconsin statute [S.943.70 (2) 4.] prohibits willfully, knowingly, and without authorization taking "possession of data, computer programs or supporting documentation".

It is not clear what behavior constitutes "taking possession of" the computer, or network, memory, or files. Perhaps the program known as "the cookie monster" is an apt example of this aberrant behavior. [105] If prosecution is to proceed under such a statute, the aid of computer scientists will be required to describe more particularly what anti-social behavior should be proscribed.

K. COMPENSATORY OR PUNITIVE DAMAGES

Only a few statutes provide for either compensatory or punitive damages resulting from the prohibited offenses, e.g. Arkansas, California, Connecticut, Delaware, Illinois, and Virginia. Arkansas provides [S. 5-41-106(a)] for recovery "for any damages sustained and the costs of the suit... 'damages' shall include loss of profits". Restitution for damages such as sustained by Aldus for the disks infected with the Peace Virus could presumably be claimed under this statute.

Connecticut provides for a fine "not to exceed double the amount of the defendant's gain from the commission of such offense" [S.53a-257], and California permits a civil suit to be brought for "compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." [S.502(e)(1)] This provision would seem to cover the Aldus virus. Although the Aldus virus caused no direct harm which might be the subject of litigation, software developers whose products were suspected to be contaminated did incur substantial expenses in verifying that no harm had occurred. However, for those companies whose products, networks, or software were not "accessed", this avenue for relief might not be adequate.

In summary, state laws seem to be quite varied (see Appendix B for analysis state by state), perhaps too diverse, for an electronic environment in which computerized networks are interconnected both nationally and transnationally. Only a few of the states seem to have addressed the question of venue (e.g. Connecticut S.53a-260; Delaware S.938; Georgia S.16-9-94; Kentucky S.434.860; South Carolina S.16-16-30; Mississippi S.97-45-11; New Hampshire S.638.19; Tennessee S.39-3-1405; Virginia S.18.1-152.10). Georgia seems to have the most comprehensive, granting jurisdiction to "any county from which, to which, through which, any access to a computer or computer network was made". The number of potentially harmful occurrences which straddle two or more jurisdictions is very likely to increase with greater computer connectivity. Thus liberalized venue statutes and jurisdictional harmonization seem highly desirable. Of the cases used herein as examples, only the Burleson case neatly falls within the jurisdiction of only one state, and several involve multiple countries; e.g. the Pakistani Brain, the Aldus Peace Virus, the Computer Chaos Club, the IBM Christmas card.

At a minimum, state legislation can be improved substantially to harmonize the behavior which is considered objectionable and to minimize the likelihood that harmful insertion of viruses will escape prosecution. Yet such legislation needs to be carefully drawn. Otherwise it may sweep up in its net the legitimate experiments of the computer novices whose ambitions to improve their skills need to be encouraged and who would benefit from access to a legitimate "electronic playground" (e.g. Mitnick never owned a computer). [62]

Overly restrictive legislation may handicap the computer professionals who need a reasonably open environment in which to develop new software and to modify it for their own purposes. Such legislation may inhibit needlessly the efforts of computer software companies to provide technological protection. Most lamentable may be the suppression of the very openness and ease of communication which computer networking has made possible. Just as the telephone system becomes more valuable with larger numbers of telephones connected, so it is with computer networks that openness is a virtue to be sought rather than to be prevented. As Clifford Stoll, who stalked the German intruders, has so eloquently stated:

> An enterprising programmer can enter many computers, just as a capable burglar can break into many homes. It is an understandable response to lock the door, sever connections, and put up elaborate barriers. Perhaps this is necessary, but it saddens the author, who would rather see future networks and computer communities built on honesty and trust. [104]

Some computer scientists [38] believe that more robust computer systems can be designed which will withstand the invasions of rogue computer programs without diminishing the user friendliness of the electronic environment.

The current challenge is whether or not adequate laws can be written to prohibit behavior which endangers the integrity of computer networks and systems without inhibiting the ease of use which is so desirable.

VI. FEDERAL STATUTES

According to published reports, federal prosecutors considered many possible offenses for which the perpetrator of the INTERNET worm might have been indicted under Title 18 of the U.S. Code. These included among others:

Section 1029 -	Fraud and Related Activity in Connection with Access Devices
Section 1030 -	The Computer Fraud and Abuse Act
Section 1343 -	Fraud by wire, radio, or television
Section 1346 -	Scheme or Artifice To Defraud
Section 1362 -	Malicious Mischief - directed toward government property
Section 2510 -	The Electronic Privacy Act of 1986
Section 2701(a) -	Unlawful Access to Stored Communications

Section 1029 defines an "access device" to include "other means of account access that can be used to obtain money, goods, services, or any other thing of value..." but the device must be used "knowingly and with intent to defraud".

The expectation had been that Section 1030 would be the appropriate statutory authority. The Computer Fraud and Abuse Act is directed primarily toward unauthorized and intentional access to classified government data, financial data, or interference with the use of federal agency computers. Section 1030(a)(4) requires an intent to defraud by unauthorized use of a "federal interest" computer (defined to include computers accessed from more than one state). Section 1030(a)(5) provides coverage in the case of intentionally preventing or interfering with authorized use of a federal interest computer but couples that with a "loss" of $1000 or more. This was the only section of the act cited in the indictment of RTM. [117] Careful analysis still suggests that it may be difficult to prove "beyond a reasonable doubt" either intent, direct damage, or exceeding authorized use.

Many computer scientists and some lawyers now conclude that releasing a computer virus is per se malicious. Indeed, Congressman Herger, in announcing his sponsorship of H.R. 55, described a virus as "a malicious program that can destroy or alter the electronic commands of a computer". The media has contributed to this conception by defining a computer virus as "an agent of infection, insinuating itself into a program or disk and forcing its host to replicate the virus code." [92]

On the other hand, others argue that a virus not only can be benign in its consequences -- as for example, the Aldus peace virus, which merely appeared on the screen and then destroyed itself -- but also that one can produce a virus with both good intentions and good effects. For example, one could imagine a self-replicating program intended to update the FBI's 10 most wanted list in all files existing for that purpose, while deleting outmoded material and not affecting any other files or applications. In this mode a "virus" becomes an automatic tool for "broadcasting" file updates to all members of a user set of unknown size, with user consent to this behavior. Hebrew University used a computer virus to identify and delete the Friday, the thirteenth virus, which was detected there prior to the date on which it was to release its killer capabilities. [41]

Furthermore, the Xerox Corporation at its Research Park in Palo Alto has been experimenting with benign uses of computer viruses for some years. [110] Several types of worm programs were developed which could harness the capabilities of multiple computers linked by communications lines into extended networks, thereby coordinating the operations, maximizing the efficiency, and increasing the output of the network. [96a] In effect, the sum of the whole could be greater than its parts, according to computer consultant John Clippinger. In the words of John Shoch, who coordinated the research for Xerox, new programming techniques were developed which could "organize complex computations by harnessing multiple machines." The various utilitarian applications included bulletin boards which distributed graphics, e.g. a cartoon a day to ALTO computer users, alarm clock programs which scheduled wake up calls or reminders, multiple machine controllers, and diagnostic worms which would seek out available computers and load them with test programs. [97a] Thus the placement of a rogue program into a computer network or operating system or program is not necessarily done with malicious intent.

Section 1346 was enacted to insure that a scheme or artifice to defraud includes depriving "another of the intangible right of honest services" which would cover the behavior of the INTERNET worm. Yet the scheme must still have been devised with intent to defraud, which is not easily established by incontrovertible evidence.

Section 1362 is directed toward willful or malicious injury to or destruction of property including "other means of communication" controlled by the U.S. government and including "obstructs, hinders, or delays the transmission over any such line..."

Section 2510 adds "electronic communication" after "wire" and defines electronic communication as (12) "...any transfer of signs, signals, writing, images, sounds data, or intelligence of any nature..." and electronic communications service as "...any service which provides to users the ability to send or receive...electronic communications". Rogue programs, such as the INTERNET worm, if inserted either without authorization or in excess of authorized use, arguably could constitute a prohibited invasion of electronic privacy in an electronic mail system. [85a]

The delay by federal prosecutors of more than six months after the INTERNET worm incident prior to an indictment suggests considerable difficulty in determining whether or how to proceed. There are a number of possibilities which justify their lengthy deliberations. These include:

(a) disagreement among the federal lawyers on the appropriate statutes under which the indictment should fall,

(b) a reluctance to prosecute a bright student,

(c) difficulty in assembling credible evidence that would withstand challenge,

(d) a doubt that intent can be proven,

(e) difficulty in proving that RTM was exceeding his authorized use,

(f) loss or destruction of crucial evidence connecting the accused with the activity prohibited, [71],

(g) lack of priority for the allocation of scarce human resources to take the case to court, given the attention demanded by drug traffic and other serious crimes,

(h) the challenge of collecting data and testimony from diverse locations or merely,

(i) extreme care in piecing together the puzzle before indicting a suspect.

Nonetheless, the delay leads thoughtful observers to deduce that the current state of the law may not be adequate to satisfactorily allay fears that electronic highways may not be safe.

VII. PROPOSED FEDERAL LEGISLATION

The Herger Bill, H.R. 55 - The Computer Virus Eradication Act of 1989 (see Appendix C), is intended to plug the gap in legislation which clearly did not anticipate viruses as one of the maladies then being addressed. The bill contains the word "virus" in the title, but does not use the word within the operative clauses. The prohibited behavior is "knowing or having reason to believe that such information or commands may cause loss, expense, or risk to health or welfare". Perhaps, after the INTERNET worm, one can no longer argue that entering a "virus" into a computer network is possible without the knowledge of almost certain harm, disruption of service, or loss of time to the operators of the system.

The operative prohibition is coupled with a clause (Paragraph B) which penalizes the perpetrator only if the program is inserted without the knowledge of the recipient. This is intended to relieve from liabilities persons who include a "time bomb" to self destruct at the end of a license period and use of viruses for study or for benign purposes known to system users. Perhaps the two phrases should have been connected with OR rather than AND. If they are coupled in this manner, however, a deleterious virus program could be inserted into a computer network with the collusion of a recipient "person". Thus the circumstances which are most prevalent might not be covered (e.g. insertion of an infectious program into a network and/or unforeseen disastrous consequences affecting third parties), although the transfer of an infected disk to an innocent party would certainly fall within the ambit of the proposed legislation.

Furthermore, there is a certain justified apprehension that disclosure to the recipient of all potential harmful consequences would, in effect, impose strict liability upon software developers to completely "debug" their software before issue or carry sufficient insurance to ward against all eventualities. Such a requirement might hamstring an industry which has been characterized by rapid innovation and close the door to small entrepreneurs who could not enter a market overburdened with burdensome insurance costs.

The MacMillan Bill, H.R. 287 (see Appendix D), entitled the Computer Protection Act of 1989, essentially addresses willful sabotage and authorizes appropriate compensatory damages to be sought. However, the proposed language does not specify what constitutes "sabotage". Thus the language may be too restricted to include such more benignly intended program "pranks" as the Aldus virus, yet may be too vague to withstand constitutional challenge.

There is more legislation to come, as William Sessions, Director of the Federal Bureau of Investigation promised to submit recommendations to Senator Patrick Leahy (Dem.-VT) at a Senate hearing held on May 15, 1989. According to Sessions, who said the agency has trained more than 500 agents for investigation of computer crimes, a team is being organized to concentrate on computer worms and viruses, for which there is no specifically applicable federal statute. [50]

VIII. NEWLY ENACTED AND PROPOSED STATE LEGISLATION

According to the best information available in mid July of 1989, several states have enacted new computer abuse legislation or are considering new computer abuse legislation. These include Alaska, California, Illinois, Maine, Maryland, Massachusetts, Michigan, Minnesota, New Mexico, New York, Oklahoma, Oregon, Pennsylvania, Rhode Island, Texas, Vermont, and West Virginia. [27]

A. MINNESOTA

The original Minnesota bill would have revised S.609.87 by adding a subdivision 11 with respect to a "destructive computer program" defined as including a "virus", a "trojan horse", a "worm", and a "bacterium". The phrase "bacterium" has not, heretofore, been used extensively in the computer science literature on the subject of rogue programs, although a few computer scientists find it a more suitable comparison with medical terminology than "virus". [34,38] Moreover, the definition of a "worm" includes the intention to "disable or degrade performance", but it is not at all obvious that the designer of the INTERNET "worm" intended to disable the networks. Rather it was the reported intention to inject a slowly self-replicating "worm" whose presence would not be obvious or easily detected, or damage other programs existing within the network. However, the definition of "destructive products" includes "producing unauthorized data that make computer memory space unavailable for authorized computer programs", thus was clearly intended to cover precisely the situation that occurred.

There was apprehension among lawyers representing computer software companies who reviewed the proposed bill that the attempt to enumerate types of rogue programs so specifically might create more problems than it solved. [33] As a consequence, the legislation, as enacted, (H.F. 647 amending Sections 609.87 and 609.88; see Appendix E) was written more broadly to describe the unacceptable consequences rather than the miscreant programs themselves:

> "Destructive computer program" means 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 product if it produces unauthorized data, including data that make computer memory space unavailable; results in the unauthorized alteration of data or computer programs; or produces a destructive computer program, including a self replicating program. (Subd. 11)

B. MARYLAND

The Maryland amendment (House Bill 1065 amending Article 37, Section 146) signed into law by the governor on May 25, 1989 [Chapter 7-22] refers to "harmful access to computers" and adds two new sections: (1) "cause the malfunction or interrupt the operation of" and (2) "alter, damage, or destroy data or a computer program". The latter phrase merely extends coverage to offenses which most of the other states already prohibit. The first term appears to be broader than the majority of the states now include and seems to cast a wide enough net to capture the INTERNET worm and the Aldus virus, as well as the Pakistani Brain.

C. WEST VIRGINIA

The West Virginia legislature has enacted in the 1989 legislative session its first computer abuse law. (Enrolled Senate Bill no. 92, see Appendix F.) According to sponsors of the legislation, enactment puts West Virginia at the forefront of states most hospitable to the computer software industry. [43] Specifically covering the introduction of a virus "that destroys the intellectual integrity of that program", it also addresses tampering and tapping as well as invasions of privacy. The bill permits equipment that is used in the commission of a crime to be confiscated and turned over to the West Virginia educational system. It also holds corporate officers accountable for illegal activities within their organizations. Thus West Virginia is one of the first states to tackle the thorny problem of reluctance of affected organizations to report to law enforcement authorities circumstances which contravene the law. However, existing statutes in Georgia [Ch.16-9-95] and Utah [Ch.76-6-705] do impose a duty to report knowledge of prohibited computer-related activities.

D. TEXAS

In Texas the Burleson case was successfully prosecuted under that state's computer crime legislation. A minor amendment was proposed to permit the confiscation of computer equipment, a sanction which is considered to be sufficiently appropriate to fit the crime to deter teenage "hackers" who cruise the computer networks looking for excitement. [80]

However, the Texas legislature passed legislation which was far more comprehensive, both defining computer viruses and prohibiting their introduction into a "computer program, computer network, or computer system". [HB 2312, passed by House on May 15 and Senate on May 25, 1989; amending Section 33.01 (9) and Section 33.03 (a) (6) of the Penal Code]. The new Texas statute also liberalizes the venue requirements [Section 13.24 (b)] and authorizes a civil right of action for damages incurred. [Section 143.001 (a)]

E. ILLINOIS

The Illinois General Assembly Legislative Research Unit has issued a report "Computer Viruses and the Law" which finds the substantive law adequate in its definitions but suggests amending Illinois statutes to reenact a now-superseded civil right of action for miscreant computer behavior in a computerized environment. [27]

The proposed legislation [AB 1153 introduced 4-7-89] offers a new offense of inserting or attempting to insert a program "knowing or having reason to believe" that it may damage or destroy.

F. PENNSYLVANIA

The Pennsylvania legislature's research report recommends that the proscribed behavior should be better defined and that the penalties prescribed should bear a better relationship to the severity and nature of the damages sustained. [61] The proposed legislation [S. 17, as amended] is arguably overreaching in its thrust as it is intended to prohibit all insertions of computer viruses into computer memories, networks, or systems, thus proscribing utilitarian as well as deleterious programs designed to replicate themselves. A computer virus is broadly defined as "a program or set of computer instructions with the ability to replicate all or part of itself..." [S. 17, amending Title 17, Section 3933 (d)].

G. NEW YORK

The New York bills [S.3560, S.5999, A.5738] purport to increase the maximum fines and years of incarceration to more nearly approximate the magnitude of the damages inflicted. These would liberalize the criteria of intent necessary for a conviction to include a reasonable knowledge that damage would result. [69] This provision would likely ease one of the problems under the federal legislation which does not take into consideration behavior considered in reckless disregard of the consequences.

H. MASSACHUSETTS

There were four bills introduced in Massachusetts in early 1989 [H.2008,H.4337,S.232,S.1701], one of which was designed explicitly to cover computer viruses. [S. 1701] The bill distinguishes between "computer larceny" comprised of "knowingly" releasing a computer virus that "destroys or modifies data" and "computer breaking and entering" which covers a computer virus which "does interfere with the user's ability to the use of the computer" but neither destroys nor modifies data. There are three levels of fines and imprisonment offered according to the level of interference (maximum $500 and/or not more than one year), modification ($750 and/or not more than one year), or destruction of data ($25,000 and/or up to 10 years.)

The other three bills are general purpose computer crime and abuse statutes which would bring Massachusetts into line with the majority of the other states which have such coverage.

I. CALIFORNIA

The California legislature received four bills between January and March 1989 [A.1858 and A.1859, S.304 and S.1012]. S.1012 was intended to increase the penalties for existing infringements of the law which include "tamper", "damage" and "access without authorization". A. 1858 was addressed to extradition, expanding the circumstances under which extradition could be requested and adding Section 1548.4 which includes the following:

> However, the demand or surrender on demand may be made even if the person whose surrender is demanded was not in the demanding state at the time of the commission of the crime and has not fled from the demanding state...or at the time of the commission of the crime was in the demanding state.

This was clearly intended to cover the situations involved with computer networks where the perpetrator of the act which injures parties or equipment within the demanding state was in another jurisdiction at the time of the act in question.

S. 304 and A. 1859 are companion bills designed to cover the computer rogue programs which are generically referred to as "computer contaminants". The operative language [Section 502(a)(10)] reads as follows:

> "Computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network

> without the intent or permission of the owner of the information. Computer contaminants include, but are not limited to, a group of computer instructions commonly called "viruses" or "worms" that are self replicating or self propagating and are designed to consume computer resources, modify, destroy, record, or transmit data or in some other fashion usurp the normal operation of the computer, computing system, or computer network.

The act prohibited is knowingly introducing a computer contaminant into a computer network or system without the specific approval of the proprietor. [Section 502(c)(8)].

Other more questionable provisions provide for exclusion from employment with computers [Section 502(e)(3)] and suspending the awarding of degrees by California colleges and universities [Section 502(e)(4)], a sanction also proposed in New York [S.599 adding a new section 156.55]. Moreover, the amendment proposes to impose a duty on those knowledgeable about acts related to computer abuse within their purview to report such violations to law enforcement authorities. [Section 502(1)] This would eliminate a major problem which is the failure of employers to bring incidents to the attention of the authorities.

J. NEW MEXICO

In New Mexico, a greatly expanded Computer Virus Act is under consideration [S.482 amending Chapter 215]. In addition to a more comprehensive coverage of "unauthorized computer use", the major thrust is toward forfeiture of equipment used to accomplish the prohibited acts. As effective as this may be in deterring miscreants who own their equipment, it would have no impact on "hackers" such as RTM or "technopaths" such as Mitnick who used computer resources belonging to third parties.

IX. TRENDS IN RECENT LEGISLATIVE ACTIVITY

The spate of legislative initiatives taken in states with a preponderance of economic activity in the computer equipment and software industries, especially California, Massachusetts, New York, and Minnesota, suggests that existing statutes are not seen to be entirely satisfactory for the prosecution of perpetrators of destructive rogue computer programs. Even in states where the statutes may be presently adequate, such as California, refinements are sought to make infringements which endanger the health of computer networks and systems easier to prosecute.

A. DEFINITIONS

The most important trend is in defining more precisely the activities to be prohibited. These include such terms as:

-- "take possession of" meaning to exert control over a computer network or system [Mass. H. 4337]

-- "tampers with" [Massachusetts, H. 2008; Vermont H.66, Sec. 3852(1)]

-- "degrades", or "disables", [Minnesota HF 647]

-- "disrupts or causes the disruption of computer services or denies or causes the denial of computer services" [New York S.232 Section 3 (5)]

-- "disrupts or degrades or causes the disruption or degradation of computer services..." [West Virginia S.61-3c-8]

-- "disrupts or causes the disruption of computer services or denial of computer services" [Massachusetts S. 232, S.(3)(5)]

-- "interrupt the operation" or "cause the malfunction" [Maryland, H.B. 1065, 91r0964]

-- "self replicating or self propagating and are designed to contaminate...," "consume computer resources" or "usurp the normal operation of the computer" [California, S.B. 304 (10)]

-- "inserts a computer virus" [Pennsylvania S.17, amending Title 18, Section 3933 (4); New York, S.5999 proposing to amend Section 156.00 to add new section (7)].

B. INTENT

The showing of express intent to do harm has proven elusive in many of the incidents involving rogue computer programs, which, however unintentionally, do inflict economic costs even upon those who must verify that no harm has been done. Thus the tendency to substitute or add "knowingly" or "willfully exceeds the limits of authorization". However, it is not clear what the difference is between "knowingly" and "intentionally" since either can be interpreted to be with knowledge that harm may result, and "reckless disregard for the consequences" may imply an intent to disregard the harm which may be caused by the act in question.

C. MAKING THE PUNISHMENT FIT THE CRIME

In several instances we have seen an increase in the fines to be levied or the imprisonment to be imposed. New York has proposed the most stringent limits with a sliding scale which measures the punishment according to the amount of damage incurred. Thus "computer tampering in the first degree" involves damages exceeding $1 million from altering or destroying data or programs [new Section 156.28] in which case the judge can order reparations up to $100 thousand. [Section 6 (a) of S.3560 and A.5738]

The authorization for confiscation of equipment used to commit an offense would appear to be designed to deter teenage offenders whose activities are primarily pranks or voyeurism.

D. DAMAGES

Rather than or perhaps in addition to fines and imprisonment there is a trend toward authorizing restitution to the victim, compensatory and punitive damages, measuring the damages by loss of profits and adding the costs of verification that no damage has occurred. [e.g. Virginia, 18.2-152.12]

E. EXTRADITION

Modifying the extradition statutes to permit requests of offenders even though they have no direct involvement within the state's boundaries seems a likely trend as computer networking proliferates throughout the United States and abroad. Indeed, extradition treaties may need to be amended to reflect the realities of criminal offenses which originate in one country but have their ultimate effects perceived far beyond the country of origin.

F. VENUE

The jurisdiction within which a case may be tried is determined by the venue statutes which require a substantial relationship to the place where the prohibited behavior occurred. Although modifying the venue statutes, as in Georgia, to cover network behavior which has deleterious consequences within the jurisdiction, does not solve the problem of gaining service upon an offender, it does facilitate forum shopping to determine where best to litigate an interstate infraction of the laws. In three of the cases analyzed, (all except the "Burleson revenge"), interstate or international implications were evident. In the "Pakistani Brain" case the perpetrators were in Pakistan and the victims were primarily in the United States. In the "Aldus Peace Virus" case, the perpetrators were in both Canada and the United States, the victims in both and the injured companies in two different states within the United States.

A substantial number of states already have enacted liberal venue statutes to encompass computer networks. [Arkansas 5-41-105, Georgia 16-9-94, Kentucky 434.860, New Hampshire 638.19, New Jersey 2A:38A-6, Mississippi 97-45-11, South Dakota 43-43B-8, Tennessee 39-3-1405, and Virginia 18.2-152.10]

G. EXEMPTIONS

Just as Kentucky recognized in its exemption of unauthorized access by voyeurs who caused no damage, some states are beginning to see the implications of excessive criminalization. For example, Massachusetts [S. 232 Section 8.3] exempts employees who purloin time using computers or programs outside the scope of their employment if no injury occurs and the value of the time is less than $100.00. West Virginia has specifically excluded those who have reasonable ground to believe they had the authority or right to do what otherwise would be an offense. [Section 61-3C J(v)]

X. PROBLEMS ENCOUNTERED

There are a number of problems which will be encountered as legislators and lobbyists confront the amendment of existing statutes or try to fashion new ones applicable to the computer rogue programs.

1) Whether to be generic or specific in the description of the afflictions?

2) How to avoid overreaching prohibitions which may inhibit innovation?

3) How to assess damages, especially in instances where the perpetrators are judgment proof?

4) Whether to impose strict liability upon the providers of computer systems, services, and networks?

5) Whether to impose strict accountability to employers to report their experiences with rogue programs and to identify perpetrators?

6) Whether the imposition of too strict criminal sanctions will encourage a "user unfriendly" environment and discourage the use of computer systems and networks?

7) How to handle litigation involving multiple jurisdictions?

XI. ALTERNATIVES TO CRIMINAL STATUTES

There are, of course, alternatives to the enactment of criminal statutes. These include:

1) Establishment of higher standards of ethical values within the user communities.

2) Better computer security -- e.g. passwords, protocols, closing of "trap doors".

3) Strict liability of providers of computer services established by contract.

4) Product liability laws applied to software.

5) More anti-viral software -- At least 25 companies produce "vaccines" at the present time. [21]

6) Compulsory insurance or pooled insurance to compensate for unanticipated losses.

7) Increased use of encryption, but this increases operating costs and inhibits the very ease of use which has characterized the systems.

8) Licensing of computer professionals [90] -- but this might risk First Amendment challenge in the same way that licensing of journalists raises questions of "chilling free speech", as the medium in which the programmers and users are operating is intended for communications. Perhaps the time has come to establish what constitutes yelling "FIRE" in a crowded theater as applied to computer communities.

XII. CONCLUSIONS

Computer viruses present new challenges to law enforcement officers and legislators, as well as computer executives, scientists, programmers, and network managers. Assuming that tighter state and federal legislation offers at least one possible antidote, there are several components to be addressed:

1) The boundaries of technological protection through encryption, protected gateways, and viral detection mechanisms.

2) The need for legal enhancement through criminal or tort laws and at which levels -- state or federal or global?

3) What kinds of audit trails are necessary to track computer misuse and abuse? And what skills are needed to conduct the audits?

4) What evidence is required to prove a case in court, assuming that a litigable event has taken place?

5) What level of insurance should be adequate to guard against unforeseen disasters and whether there should be some kind of federally insured scheme similar to the Federal Deposit Insurance Corporation?

6) What standards of care should be exercised by operators or providers of computer equipment, networks, and services? Should such standards be established by private groups or by state or federal law?

In summary, it is difficult to determine strategies since it cannot be ascertained whether the rogue programs are a transient problem which will go away as "hackers" develop a different ethical standard, whether they are a drop in the bucket of problems which may arise as the criminally motivated become more computer literate, or whether they are like the common cold, afflictions which come with the use of computers with which we must learn to live.

APPENDICES

Appendix A

Viruses which Affect PC-DOS/MS-DOS

Names	Minimum No. of Strains	Type*	First Appearance
1. Brain, Pakistani	7	Boot sector	1/86
2. Merritt, Alameda, Yale	7	Boot sector	4?/87
3. South African, Friday 13th	2	COM D	1987
4. Lehigh	2	COMMAND.COM	11/87
5. Vienna, Austrian	2	COM D 648	12?/87
6. Israeli, Friday 13th, Jerusalem	9	COM/EXE R 1813/ 1808	12/87
7. April-1-Com	1	COM R 897	1/88
8. April-1-Exe	1	EXE R 1488	1/88
9. Ping-Pong, Bouncing Ball, Italian	2	Boot sector	3/88
10. Dos-62, Unesco	2	COM D	4/88
11. Marijuana, Stoned, New Zealand, Australian	2	Boot sector; partition record on hard disk	early 1988
12. Cascade, Autumn, Blackjack	6	COM R 1701/1704	9/88 (1987?)
13. Agiplan	1	COM 1536	10/88
14. Oropax, Music	1	COM RD 2756 to 2806	2/89
15. Venezuelan, Den Zuk, Search	6	Boot sector	early 1989?
16. dBASE	1	COM/EXE R	3/89
17. DataCrime	2?	COM D 1168 (1280?)	3/89
18. Missouri	1	?	4/89
19. Nichols	2?	Boot sector	?
20. 405	1	COM DO 405	4?/89
Total number of strains	**58**		

* **"Type" column definitions: R** = Resident in RAM; **D** = Direct (searches disks for uninfected files to infect); **O** = Overwrite (the virus overwrites the beginning of the file). The number(s) after the **R** or **D** indicate the number of bytes the virus extends the files; the number after the **O** is the number of bytes overwritten.

Source: Y. Radai, Hebrew University of Jerusalem, Dockmaster. May 16, 1989.

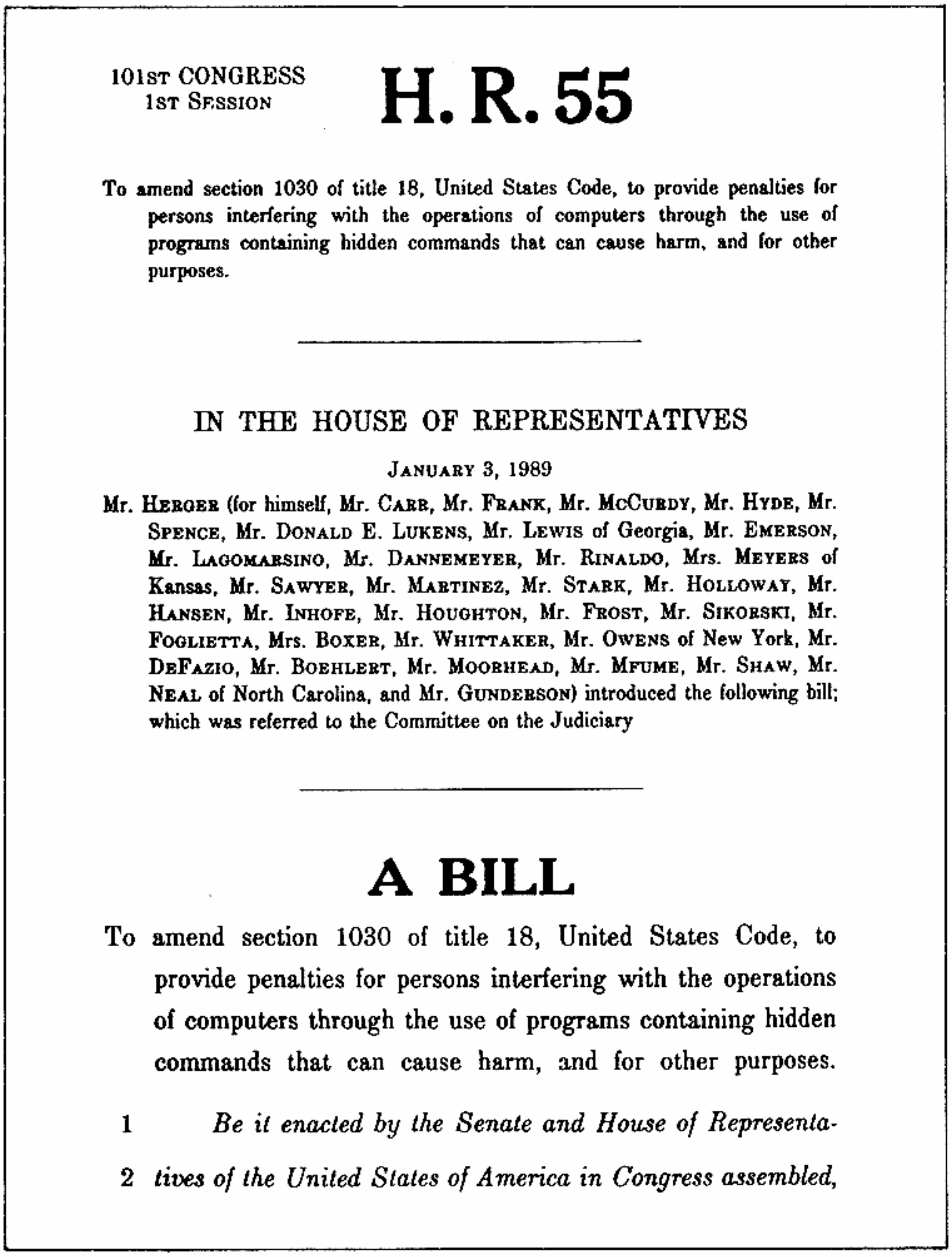
Appendix B

State Laws on Computer Crime and/or Computer Abuse

	Use Without Authority	Alter	Damage	Destroy	Block Use	Copy Files	Disclose Information	Takes	Use for Crime	Take Possession
Alabama	✔			✔			✔	✔	✔	
Alaska			✔					✔		
Arizona	✔	✔	✔							
Arkansas	✔	✔	✔	✔	✔				✔	
California	✔	✔	✔	✔	✔				✔	
Colorado	✔	✔	✔	✔					✔	
Connecticut	✔	✔	✔	✔	✔	✔	✔	✔		
Delaware	✔	✔	✔	✔	✔	✔	✔	✔		
Florida		✔		✔	✔		✔	✔	✔	
Georgia		✔	✔	✔					✔	
Hawaii	✔	✔	✔	✔					✔	
Idaho	✔	✔	✔	✔					✔	
Illinois	✔	✔	✔	✔				✔	✔	
Indiana	✔	✔	✔							
Iowa	✔		✔	✔					✔	
Kansas	✔	✔	✔	✔		✔	✔		✔	✔
Kentucky	✔	✔	✔	✔					✔	
Louisiana	✔	✔		✔	✔	✔	✔	✔		
Maine	✔									
Maryland	✔									
Massachusetts								✔		
Michigan		✔	✔	✔					✔	
Minnesota	✔		✔	✔				✔	✔	
Mississippi		✔	✔	✔	✔	✔	✔	✔	✔	
Missouri	✔	✔		✔	✔		✔	✔		
Montana	✔	✔		✔					✔	
Nebraska	✔	✔	✔	✔	✔			✔		
Nevada	✔	✔		✔	✔	✔	✔	✔		
New Hampshire	✔	✔	✔	✔	✔	✔	✔	✔		
New Jersey	✔	✔	✔	✔				✔		
New Mexico	✔	✔	✔	✔					✔	
New York	✔	✔		✔		✔		✔	✔	
North Carolina	✔	✔	✔	✔	✔				✔	
North Dakota	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Ohio	✔								✔	
Oklahoma		✔	✔	✔		✔	✔		✔	✔
Oregon	✔	✔	✔	✔					✔	
Pennsylvania		✔	✔	✔	✔				✔	
Rhode Island		✔	✔	✔				✔	✔	
South Carolina	✔	✔	✔	✔					✔	✔
South Dakota	✔	✔		✔					✔	
Tennessee	✔	✔	✔	✔					✔	
Texas	✔	✔	✔	✔	✔					
Utah		✔	✔	✔	✔				✔	
Virginia	✔	✔		✔	✔	✔		✔	✔	
Washington	✔								✔	
West Virginia	✔	✔	✔	✔	✔			✔	✔	
Wisconsin	✔	✔	✔	✔		✔	✔			✔
Wyoming	✔		✔	✔	✔					

Appendix C

The Herger Bill, H.R. 55: The Computer Virus Eradication Act of 1989



101st CONGRESS
1st Session

H. R. 55

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

IN THE HOUSE OF REPRESENTATIVES

January 3, 1989

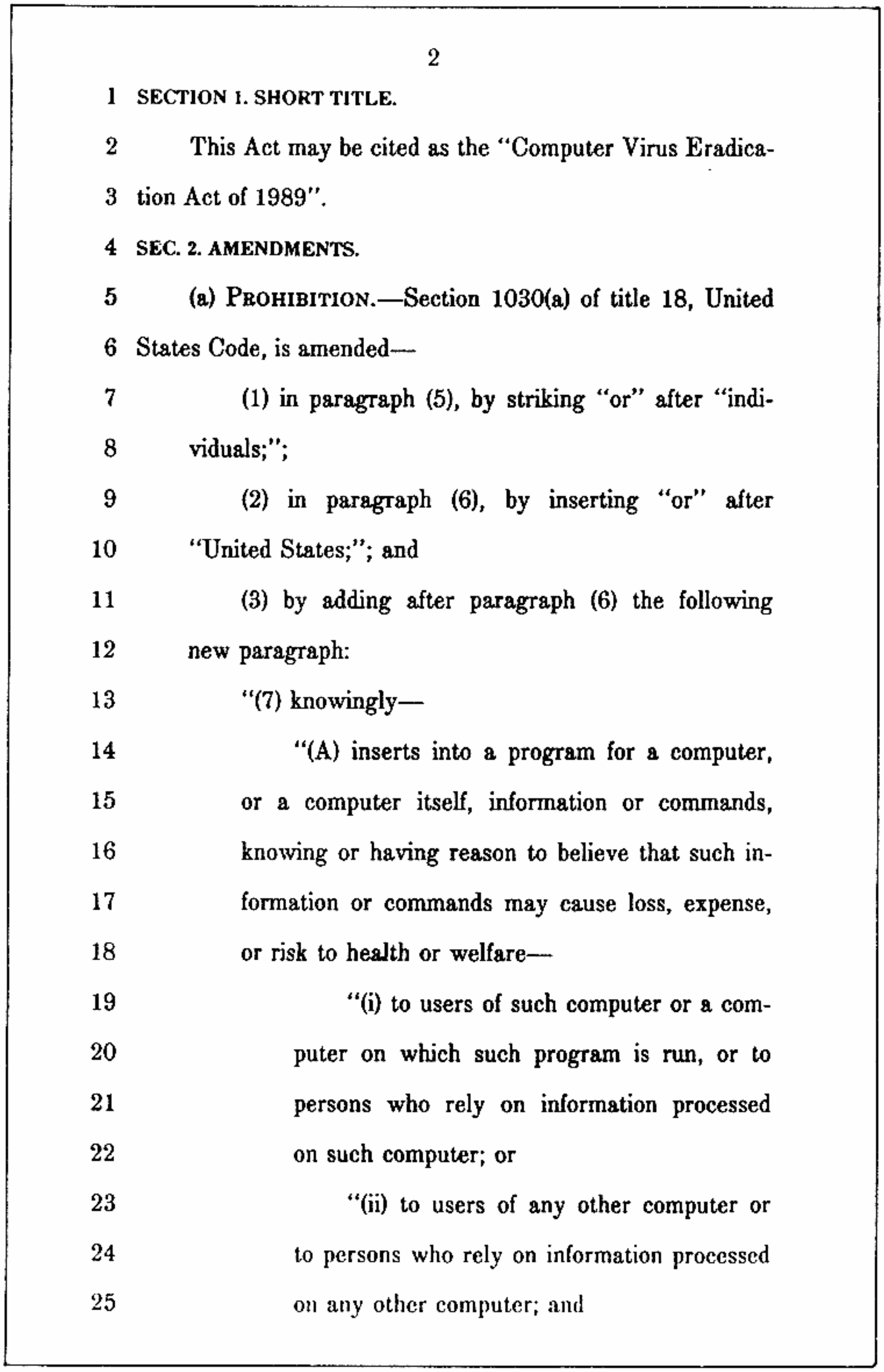
Mr. Herger (for himself, Mr. Carr, Mr. Frank, Mr. McCurdy, Mr. Hyde, Mr. Spence, Mr. Donald E. Lukens, Mr. Lewis of Georgia, Mr. Emerson, Mr. Lagomarsino, Mr. Dannemeyer, Mr. Rinaldo, Mrs. Meyers of Kansas, Mr. Sawyer, Mr. Martinez, Mr. Stark, Mr. Holloway, Mr. Hansen, Mr. Inhofe, Mr. Houghton, Mr. Frost,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

---

A BILL

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

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



SECTION 1. SHORT TITLE.

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

SEC. 2. AMENDMENTS.

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

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

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

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

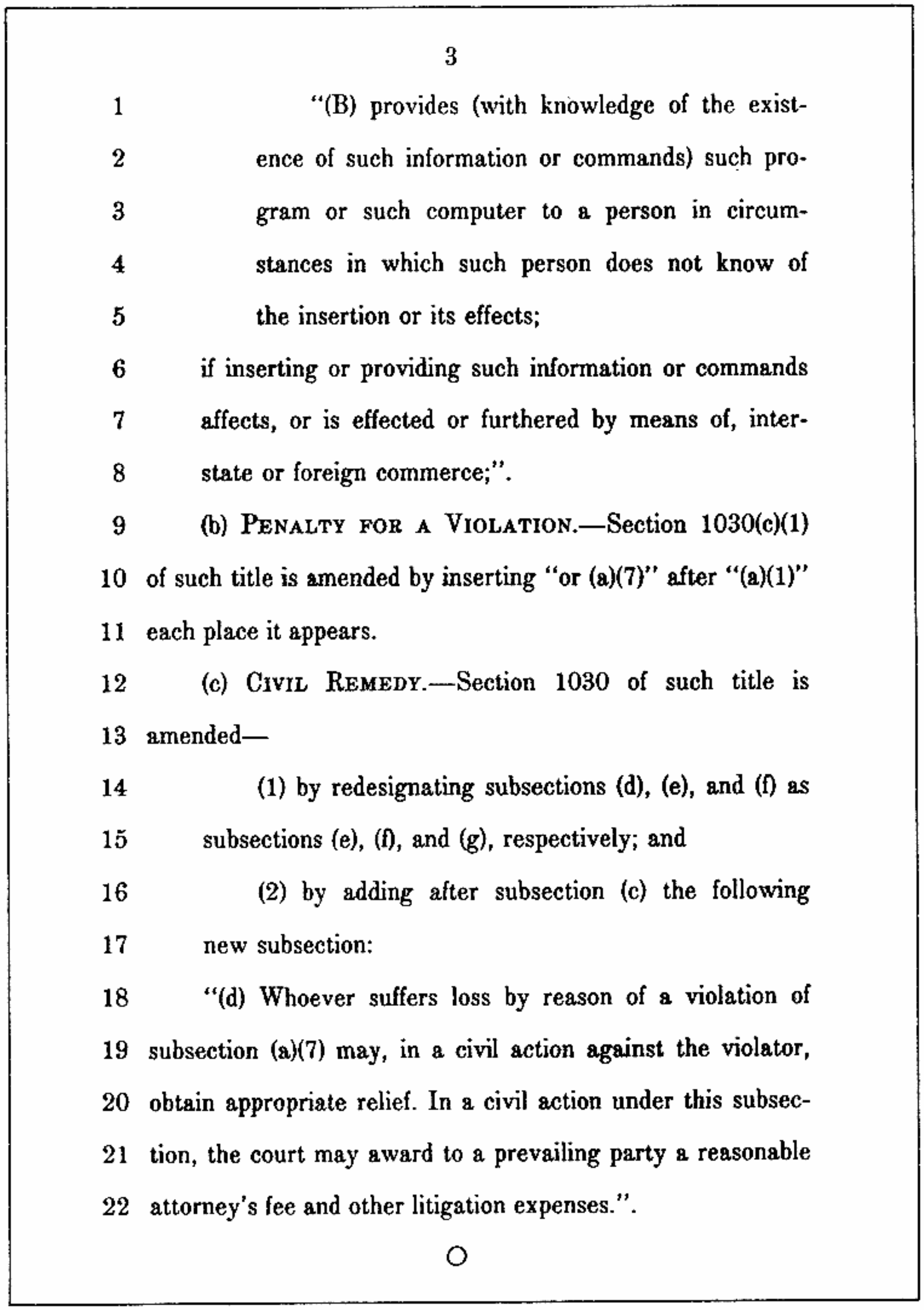
"(7) knowingly—

"(A) inserts into a program for a computer, or a computer itself, information or commands, knowing or having reason to believe that such information or commands may cause loss, expense, or risk to health or welfare—

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

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

Appendix C (continued)



"(B) provides (with knowledge of the existence of such information or commands) such program or such computer to a person in circumstances in which such person does not know of the insertion or its effects;

if inserting or providing such information or commands affects, or is effected or furthered by means of, interstate or foreign commerce;".

(b) Penalty for a Violation.—Section 1030(c)(1) of such title is amended by inserting "or (a)(7)" after "(a)(1)" each place it appears.

(c) Civil Remedy.—Section 1030 of such title is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively; and

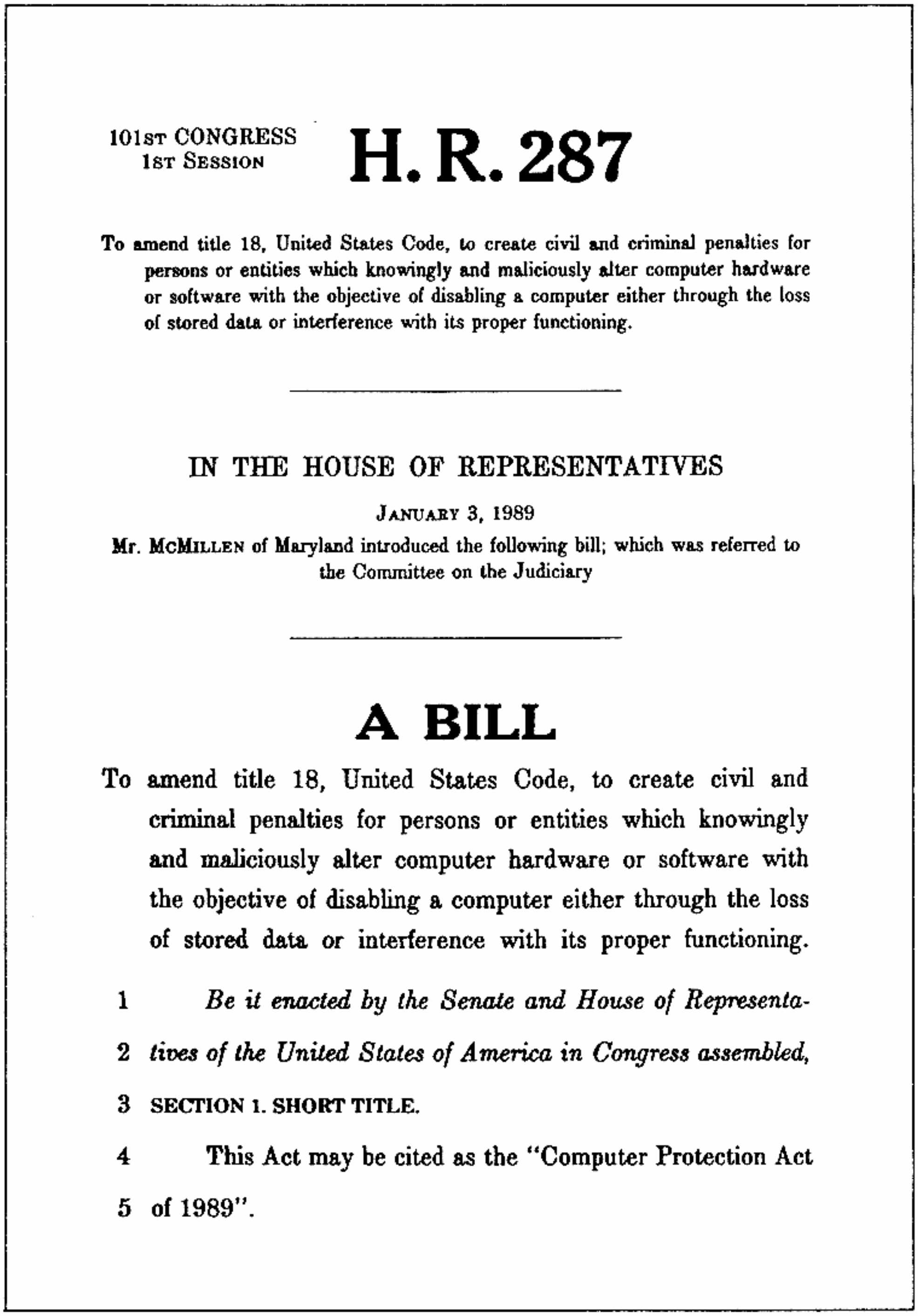
(2) by adding after subsection (c) the following new subsection:

"(d) Whoever suffers loss by reason of a violation of subsection (a)(7) may, in a civil action against the violator, obtain appropriate relief. In a civil action under this subsection, the court may award to a prevailing party a reasonable attorney's fee and other litigation expenses.".

○

Appendix D

The MacMillan Bill, H.R. 287: The Computer Protection Act of 1989



101st CONGRESS
1st Session

H. R. 287

To amend title 18, United States Code, to create civil and criminal penalties for persons or entities which knowingly and maliciously alter computer hardware or software with the objective of disabling a computer either through the loss of stored data or interference with its proper functioning.

IN THE HOUSE OF REPRESENTATIVES

January 3, 1989

Mr. McMillen of Maryland introduced the following bill; which was referred to the Committee on the Judiciary

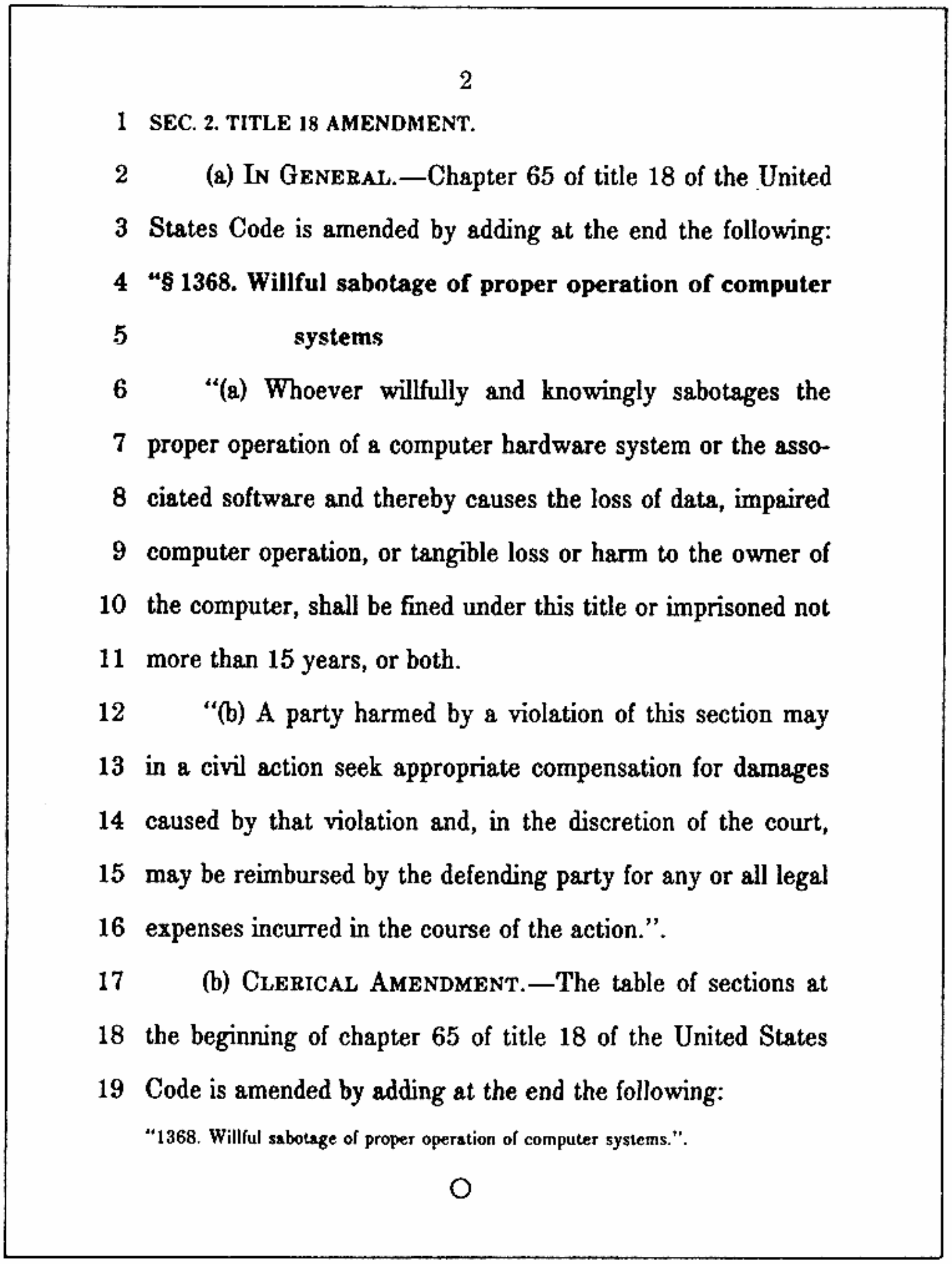
A BILL

To amend title 18, United States Code, to create civil and criminal penalties for persons or entities which knowingly and maliciously alter computer hardware or software with the objective of disabling a computer either through the loss of stored data or interference with its proper functioning.

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

SECTION 1. SHORT TITLE.

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



SEC. 2. TITLE 18 AMENDMENT.

(a) IN GENERAL.—Chapter 65 of title 18 of the United States Code is amended by adding at the end the following:

"§ 1368. Willful sabotage of proper operation of computer systems

"(a) Whoever willfully and knowingly sabotages the proper operation of a computer hardware system or the associated software and thereby causes the loss of data, impaired computer operation, or tangible loss or harm to the owner of the computer, shall be fined under this title or imprisoned not more than 15 years, or both.

"(b) A party harmed by a violation of this section may in a civil action seek appropriate compensation for damages caused by that violation and, in the discretion of the court, may be reimbursed by the defending party for any or all legal expenses incurred in the course of the action.".

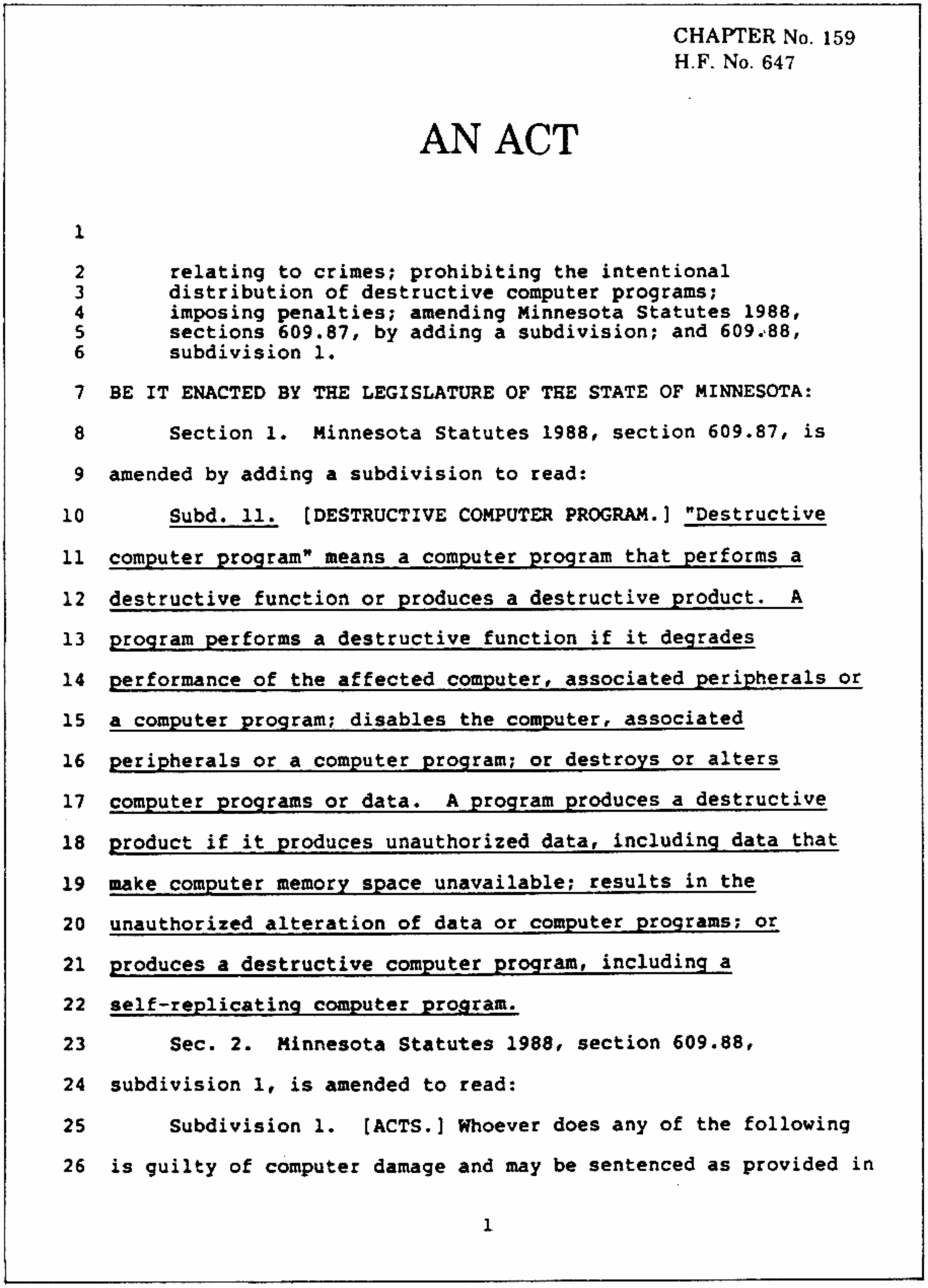
(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 65 of title 18 of the United States Code is amended by adding at the end the following:

"1368. Willful sabotage of proper operation of computer systems.".

○

Appendix E

H.F. 647 amending Minnesota Statutes 1988, Sections 609.87 and 609.88



CHAPTER No. 159
H.F. No. 647

AN ACT

relating to crimes; prohibiting the intentional distribution of destructive computer programs; imposing penalties; amending Minnesota Statutes 1988, sections 609.87, by adding a subdivision; and 609.88, subdivision 1.

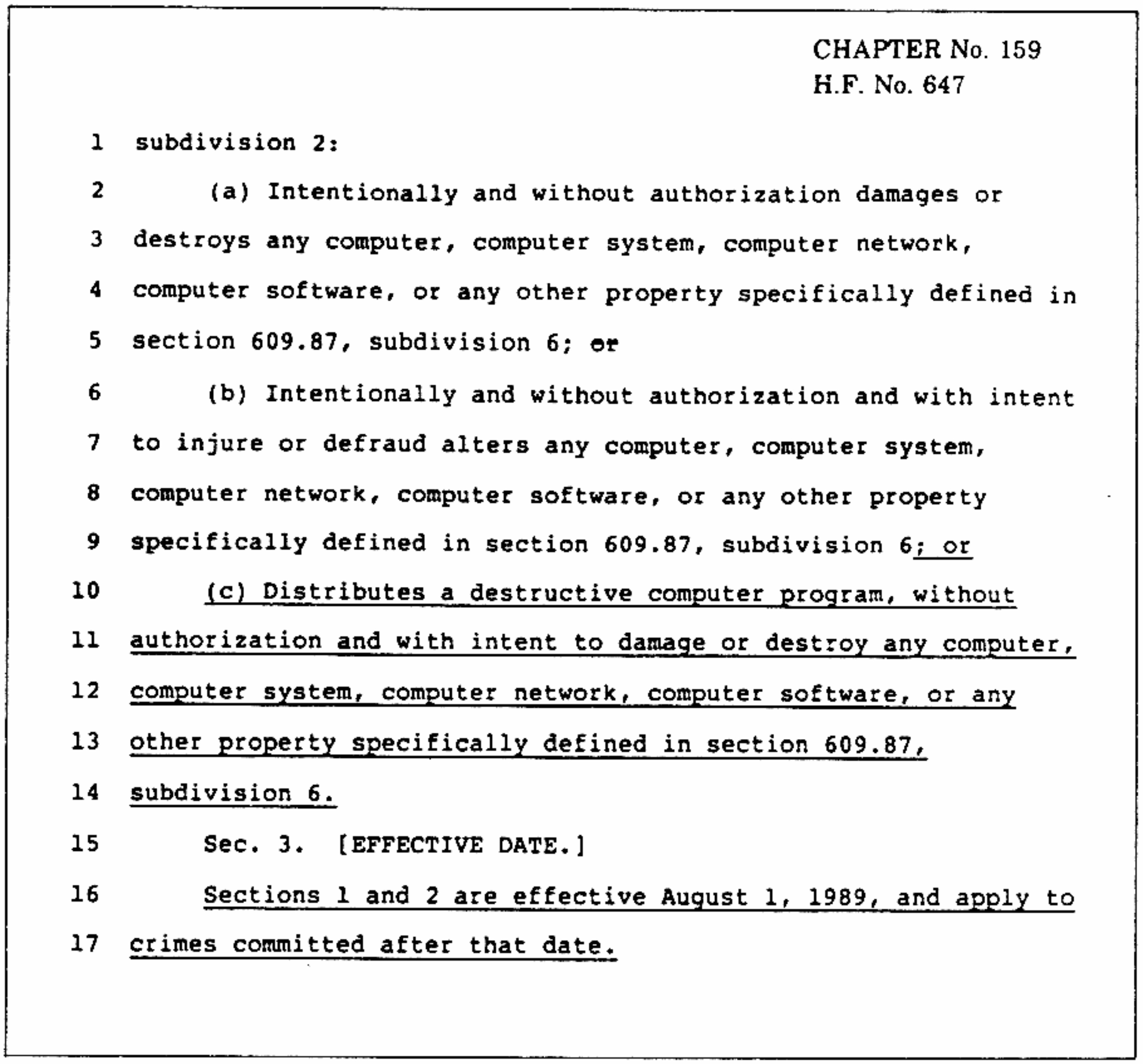
BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 1988, section 609.87, is amended by adding a subdivision to read:

Subd. 11. [DESTRUCTIVE COMPUTER PROGRAM.] "Destructive computer program" means 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 product if it produces unauthorized data, including data that make computer memory space unavailable; results in the unauthorized alteration of data or computer programs; or produces a destructive computer program, including a self-replicating computer program.

Sec. 2. Minnesota Statutes 1988, section 609.88, subdivision 1, is amended to read:

Subdivision 1. [ACTS.] Whoever does any of the following is guilty of computer damage and may be sentenced as provided in



CHAPTER No. 159
H.F. No. 647

subdivision 2:

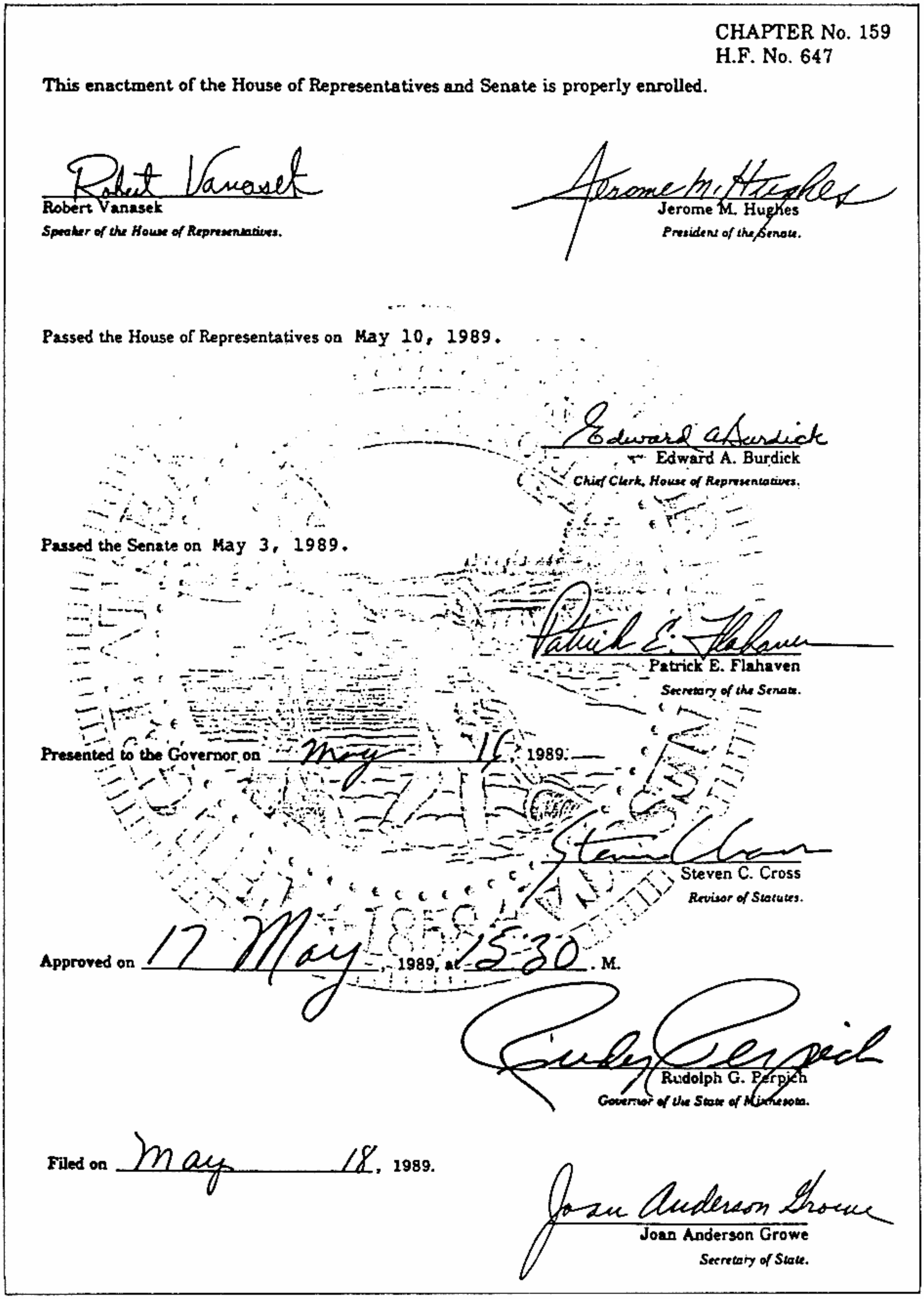
(a) Intentionally and without authorization damages or destroys any computer, computer system, computer network, computer software, or any other property specifically defined in section 609.87, subdivision 6; ~~or~~

(b) Intentionally and without authorization and with intent to injure or defraud alters any computer, computer system, computer network, computer software, or any other property specifically defined in section 609.87, subdivision 6; or

(c) Distributes a destructive computer program, without authorization and with intent to damage or destroy any computer, computer system, computer network, computer software, or any other property specifically defined in section 609.87, subdivision 6.

Sec. 3. [EFFECTIVE DATE.]

Sections 1 and 2 are effective August 1, 1989, and apply to crimes committed after that date.



CHAPTER No. 159
H.F. No. 647

This enactment of the House of Representatives and Senate is properly enrolled.

Robert Vanasek
Robert Vanasek
Speaker of the House of Representatives.

Jerome M. Hughes
Jerome M. Hughes
President of the Senate.

Passed the House of Representatives on May 10, 1989.

Edward A. Burdick
Edward A. Burdick
Chief Clerk, House of Representatives.

Passed the Senate on May 3, 1989.

Patrick E. Flahaven
Patrick E. Flahaven
Secretary of the Senate.

Presented to the Governor on May 16, 1989.

Steven C. Cross
Revisor of Statutes.

Approved on 17 May, 1989, at 15:30 M.

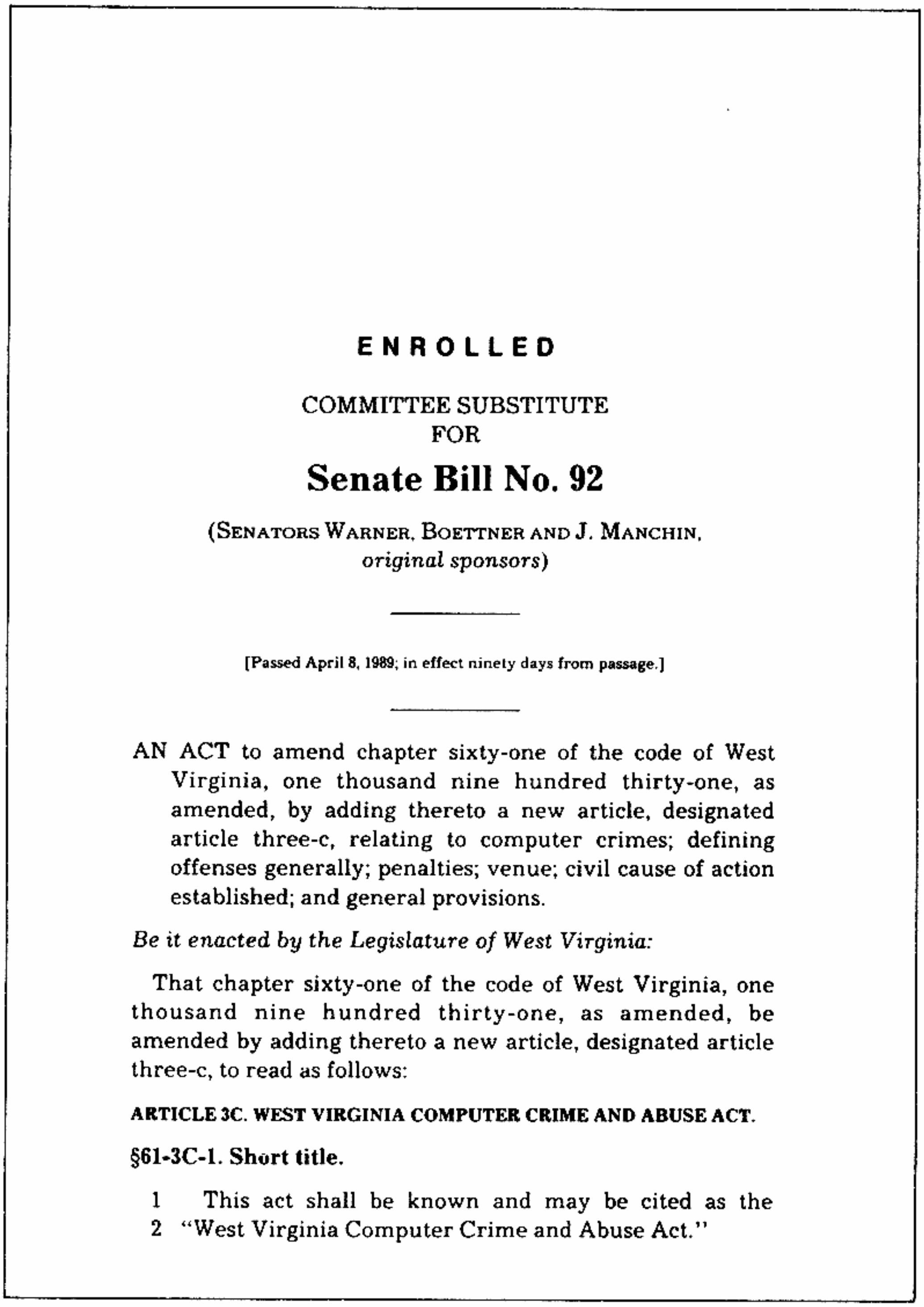
Rudy Perpich
Rudolph G. Perpich
Governor of the State of Minnesota.

Filed on May 18, 1989.

Joan Anderson Growe
Joan Anderson Growe
Secretary of State.

Appendix F

West Virginia Computer Crime and Abuse Act, Senate Bill No. 92



ENROLLED

COMMITTEE SUBSTITUTE
FOR

Senate Bill No. 92

(SENATORS WARNER, BOETTNER AND J. MANCHIN,
original sponsors)

[Passed April 8, 1989; in effect ninety days from passage.]

AN ACT to amend chapter sixty-one of the code of West Virginia, one thousand nine hundred thirty-one, as amended, by adding thereto a new article, designated article three-c, relating to computer crimes; defining offenses generally; penalties; venue; civil cause of action established; and general provisions.

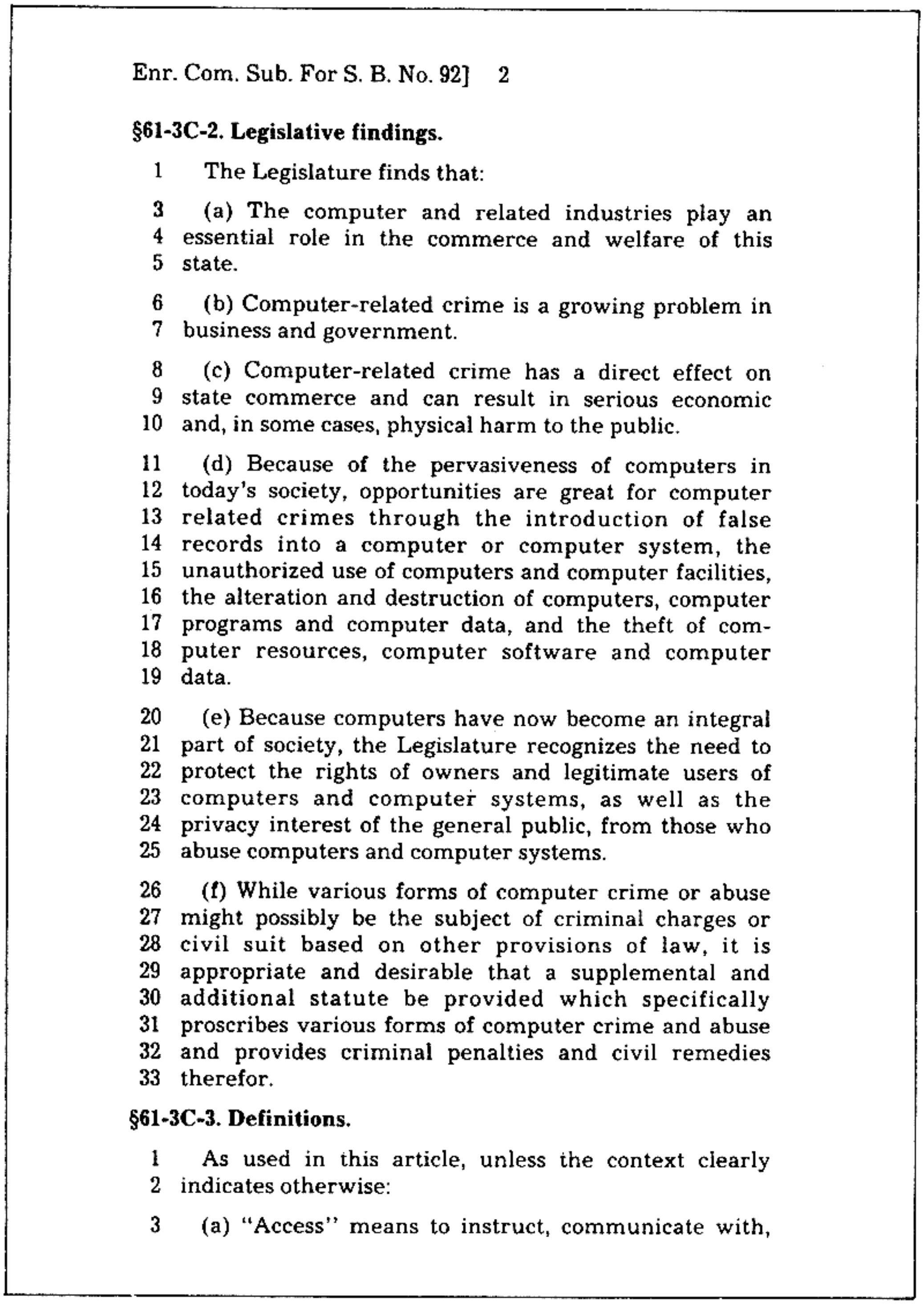
Be it enacted by the Legislature of West Virginia:

That chapter sixty-one of the code of West Virginia, one thousand nine hundred thirty-one, as amended, be amended by adding thereto a new article, designated article three-c, to read as follows:

ARTICLE 3C. WEST VIRGINIA COMPUTER CRIME AND ABUSE ACT.

§61-3C-1. Short title.

This act shall be known and may be cited as the "West Virginia Computer Crime and Abuse Act."



Enr. Com. Sub. For S. B. No. 92] 2

§61-3C-2. Legislative findings.

The Legislature finds that:

(a) The computer and related industries play an essential role in the commerce and welfare of this state.

(b) Computer-related crime is a growing problem in business and government.

(c) Computer-related crime has a direct effect on state commerce and can result in serious economic and, in some cases, physical harm to the public.

(d) Because of the pervasiveness of computers in today's society, opportunities are great for computer related crimes through the introduction of false records into a computer or computer system, the unauthorized use of computers and computer facilities, the alteration and destruction of computers, computer programs and computer data, and the theft of computer resources, computer software and computer data.

(e) Because computers have now become an integral part of society, the Legislature recognizes the need to protect the rights of owners and legitimate users of computers and computer systems, as well as the privacy interest of the general public, from those who abuse computers and computer systems.

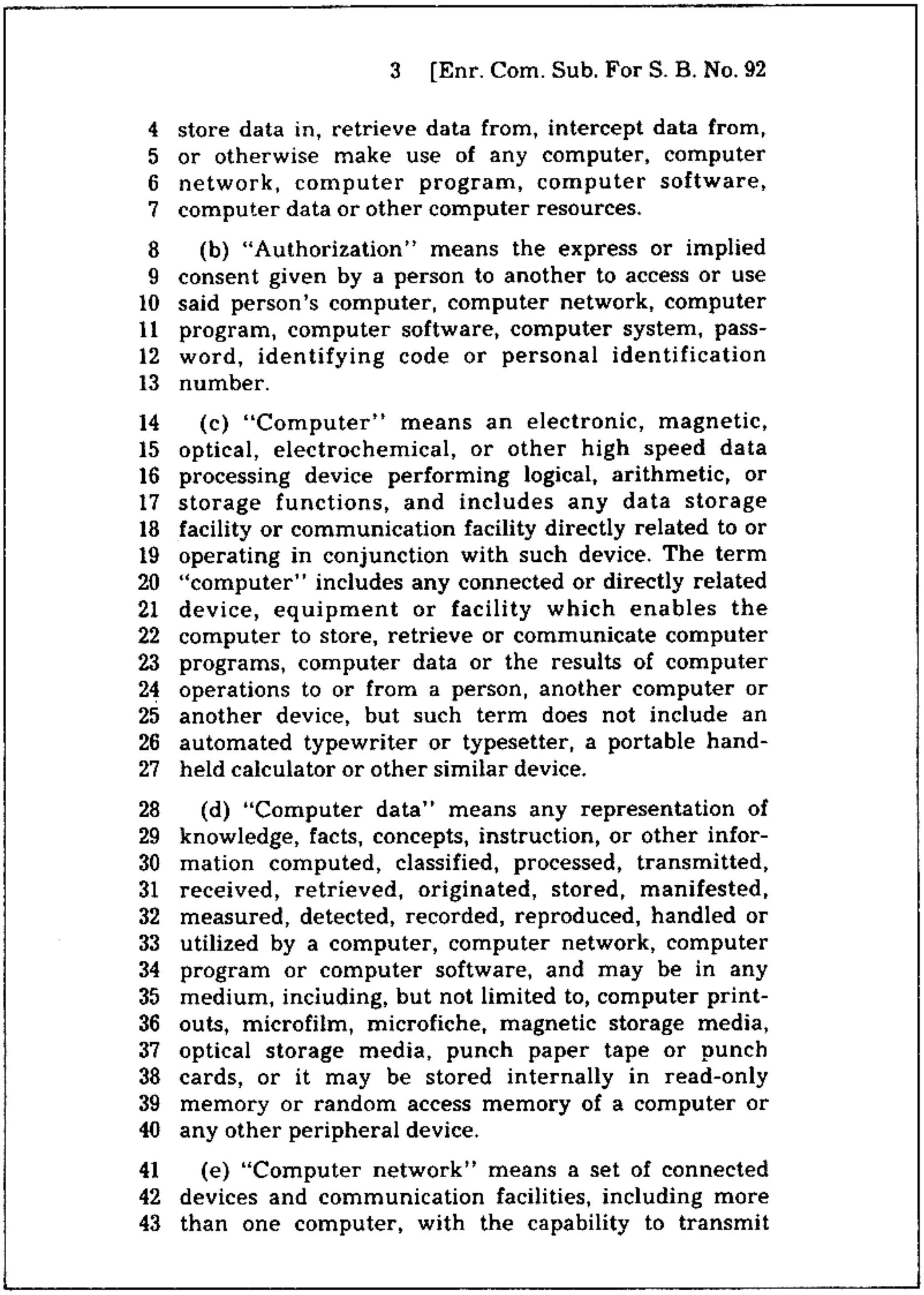
(f) While various forms of computer crime or abuse might possibly be the subject of criminal charges or civil suit based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which specifically proscribes various forms of computer crime and abuse and provides criminal penalties and civil remedies therefor.

§61-3C-3. Definitions.

As used in this article, unless the context clearly indicates otherwise:

(a) "Access" means to instruct, communicate with,

Appendix F (continued)



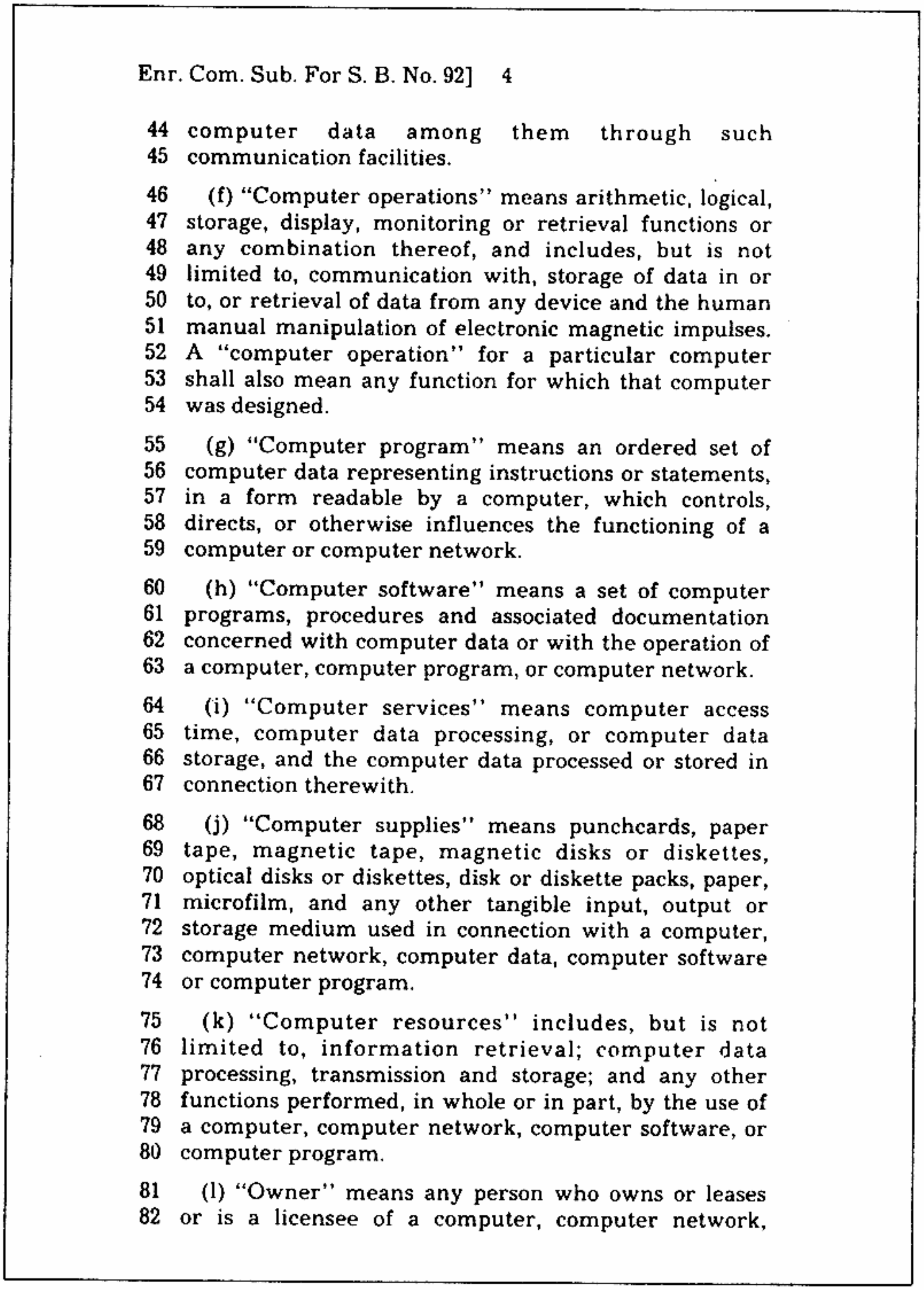
store data in, retrieve data from, intercept data from, or otherwise make use of any computer, computer network, computer program, computer software, computer data or other computer resources.

(b) "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.

(c) "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communication facility directly related to or operating in conjunction with such device. The term "computer" includes any connected or directly related device, equipment or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator or other similar device.

(d) "Computer data" means any representation of knowledge, facts, concepts, instruction, or other information computed, classified, processed, transmitted, received, retrieved, originated, stored, manifested, measured, detected, recorded, reproduced, handled or utilized by a computer, computer network, computer program or computer software, and may be in any medium, inciuding, but not limited to, computer printouts, microfilm, microfiche, magnetic storage media, optical storage media, punch paper tape or punch cards, or it may be stored internally in read-only memory or random access memory of a computer or any other peripheral device.

(e) "Computer network" means a set of connected devices and communication facilities, including more than one computer, with the capability to transmit



Enr. Com. Sub. For S. B. No. 92] 4

computer data among them through such communication facilities.

(f) "Computer operations" means arithmetic, logical, storage, display, monitoring or retrieval functions or any combination thereof, and includes, but is not limited to, communication with, storage of data in or to, or retrieval of data from any device and the human manual manipulation of electronic magnetic impulses. A "computer operation" for a particular computer shall also mean any function for which that computer was designed.

(g) "Computer program" means an ordered set of computer data representing instructions or statements, in a form readable by a computer, which controls, directs, or otherwise influences the functioning of a computer or computer network.

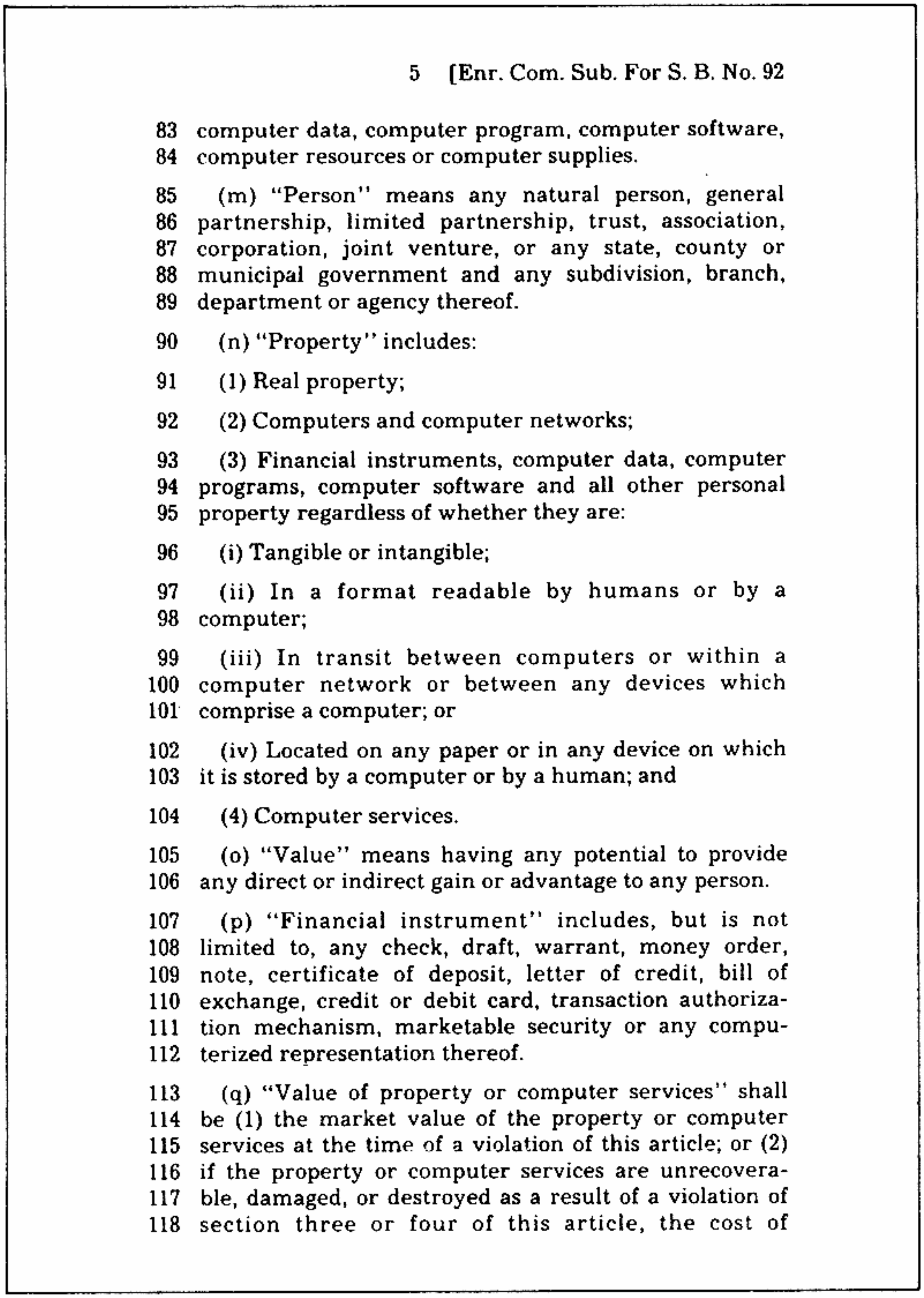
(h) "Computer software" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

(i) "Computer services" means computer access time, computer data processing, or computer data storage, and the computer data processed or stored in connection therewith.

(j) "Computer supplies" means punchcards, paper tape, magnetic tape, magnetic disks or diskettes, optical disks or diskettes, disk or diskette packs, paper, microfilm, and any other tangible input, output or storage medium used in connection with a computer, computer network, computer data, computer software or computer program.

(k) "Computer resources" includes, but is not limited to, information retrieval; computer data processing, transmission and storage; and any other functions performed, in whole or in part, by the use of a computer, computer network, computer software, or computer program.

(l) "Owner" means any person who owns or leases or is a licensee of a computer, computer network,



5 [Enr. Com. Sub. For S. B. No. 92

computer data, computer program, computer software, computer resources or computer supplies.

(m) "Person" means any natural person, general partnership, limited partnership, trust, association, corporation, joint venture, or any state, county or municipal government and any subdivision, branch, department or agency thereof.

(n) "Property" includes:

(1) Real property;

(2) Computers and computer networks;

(3) Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:

(i) Tangible or intangible;

(ii) In a format readable by humans or by a computer;

(iii) In transit between computers or within a computer network or between any devices which comprise a computer; or

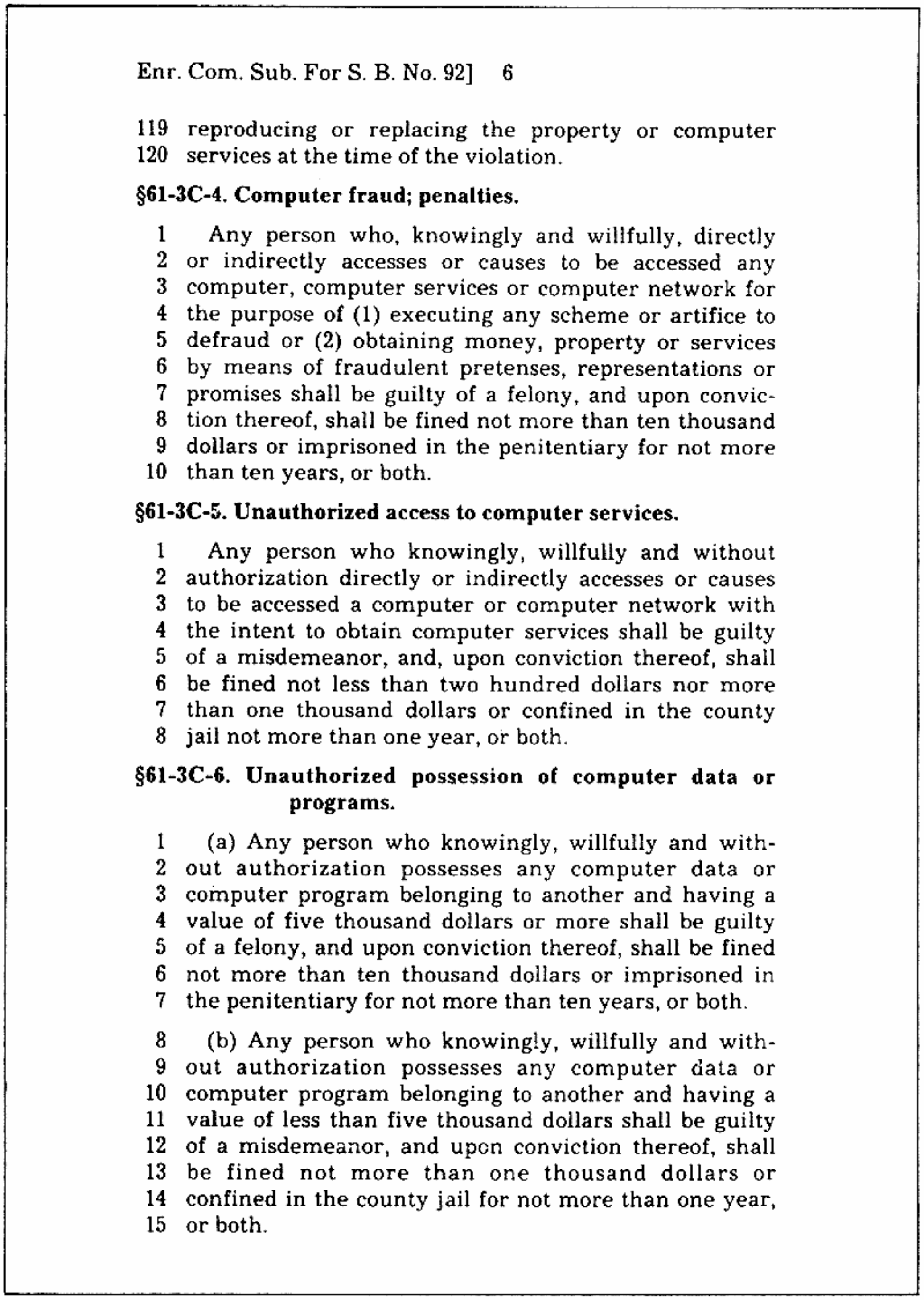
(iv) Located on any paper or in any device on which it is stored by a computer or by a human; and

(4) Computer services.

(o) "Value" means having any potential to provide any direct or indirect gain or advantage to any person.

(p) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security or any computerized representation thereof.

(q) "Value of property or computer services" shall be (1) the market value of the property or computer services at the time of a violation of this article; or (2) if the property or computer services are unrecoverable, damaged, or destroyed as a result of a violation of section three or four of this article, the cost of



Enr. Com. Sub. For S. B. No. 92] 6

reproducing or replacing the property or computer services at the time of the violation.

§61-3C-4. Computer fraud; penalties.

Any person who, knowingly and willfully, directly or indirectly accesses or causes to be accessed any computer, computer services or computer network for the purpose of (1) executing any scheme or artifice to defraud or (2) obtaining money, property or services by means of fraudulent pretenses, representations or promises shall be guilty of a felony, and upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary for not more than ten years, or both.

§61-3C-5. Unauthorized access to computer services.

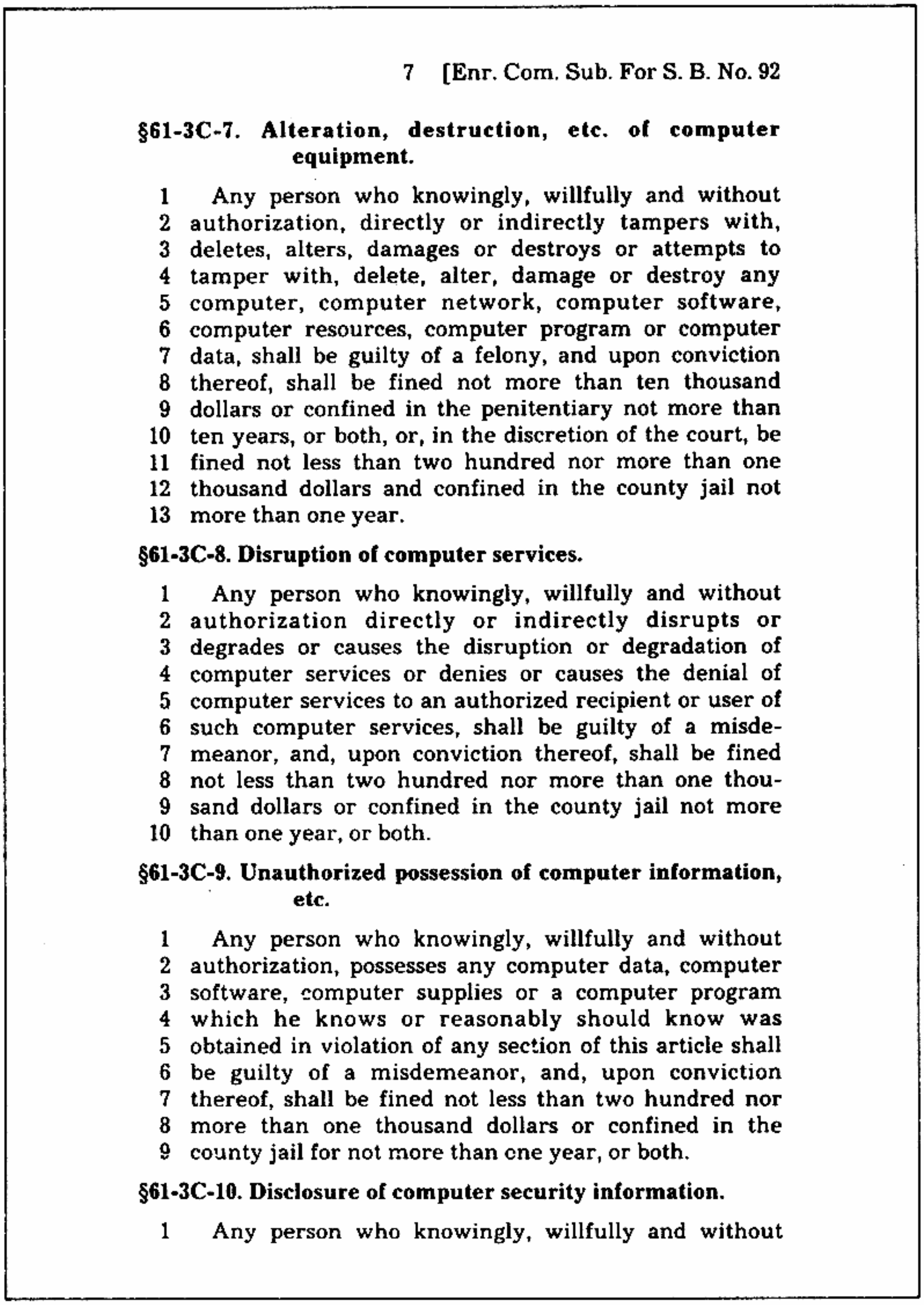
Any person who knowingly, willfully and without authorization directly or indirectly accesses or causes to be accessed a computer or computer network with the intent to obtain computer services shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred dollars nor more than one thousand dollars or confined in the county jail not more than one year, or both.

§61-3C-6. Unauthorized possession of computer data or programs.

(a) Any person who knowingly, willfully and without authorization possesses any computer data or computer program belonging to another and having a value of five thousand dollars or more shall be guilty of a felony, and upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary for not more than ten years, or both.

(b) Any person who knowingly, willfully and without authorization possesses any computer data or computer program belonging to another and having a value of less than five thousand dollars shall be guilty of a misdemeanor, and upon conviction thereof, shall be fined not more than one thousand dollars or confined in the county jail for not more than one year, or both.

Appendix F (continued)



§61-3C-7. Alteration, destruction, etc. of computer equipment.

Any person who knowingly, willfully and without authorization, directly or indirectly tampers with, deletes, alters, damages or destroys or attempts to tamper with, delete, alter, damage or destroy any computer, computer network, computer software, computer resources, computer program or computer data, shall be guilty of a felony, and upon conviction thereof, shall be fined not more than ten thousand dollars or confined in the penitentiary not more than ten years, or both, or, in the discretion of the court, be fined not less than two hundred nor more than one thousand dollars and confined in the county jail not more than one year.

§61-3C-8. Disruption of computer services.

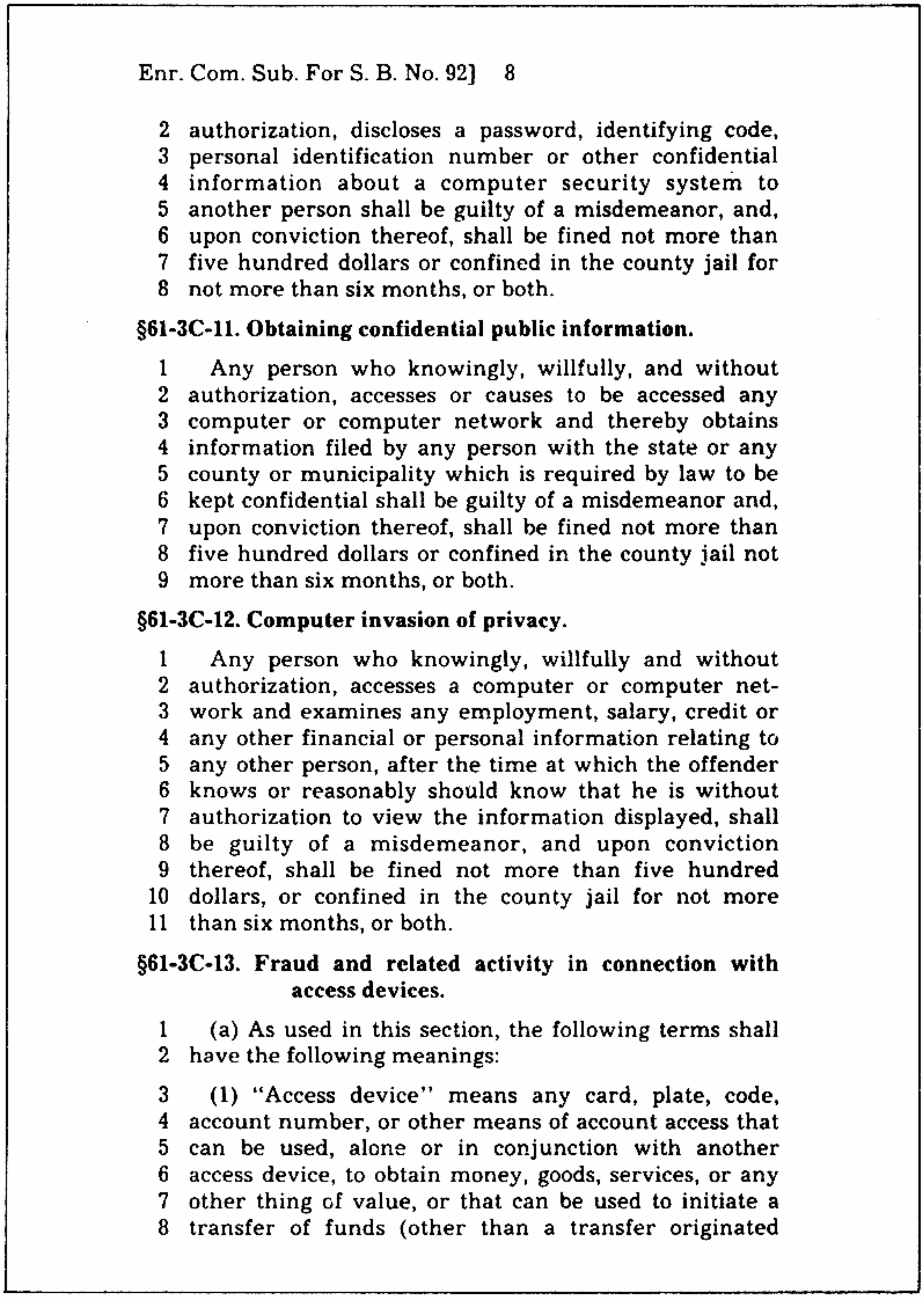
Any person who knowingly, willfully and without authorization directly or indirectly disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized recipient or user of such computer services, shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred nor more than one thousand dollars or confined in the county jail not more than one year, or both.

§61-3C-9. Unauthorized possession of computer information, etc.

Any person who knowingly, willfully and without authorization, possesses any computer data, computer software, computer supplies or a computer program which he knows or reasonably should know was obtained in violation of any section of this article shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred nor more than one thousand dollars or confined in the county jail for not more than one year, or both.

§61-3C-10. Disclosure of computer security information.

Any person who knowingly, willfully and without



authorization, discloses a password, identifying code, personal identification number or other confidential information about a computer security system to another person shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail for not more than six months, or both.

§61-3C-11. Obtaining confidential public information.

Any person who knowingly, willfully, and without authorization, accesses or causes to be accessed any computer or computer network and thereby obtains information filed by any person with the state or any county or municipality which is required by law to be kept confidential shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail not more than six months, or both.

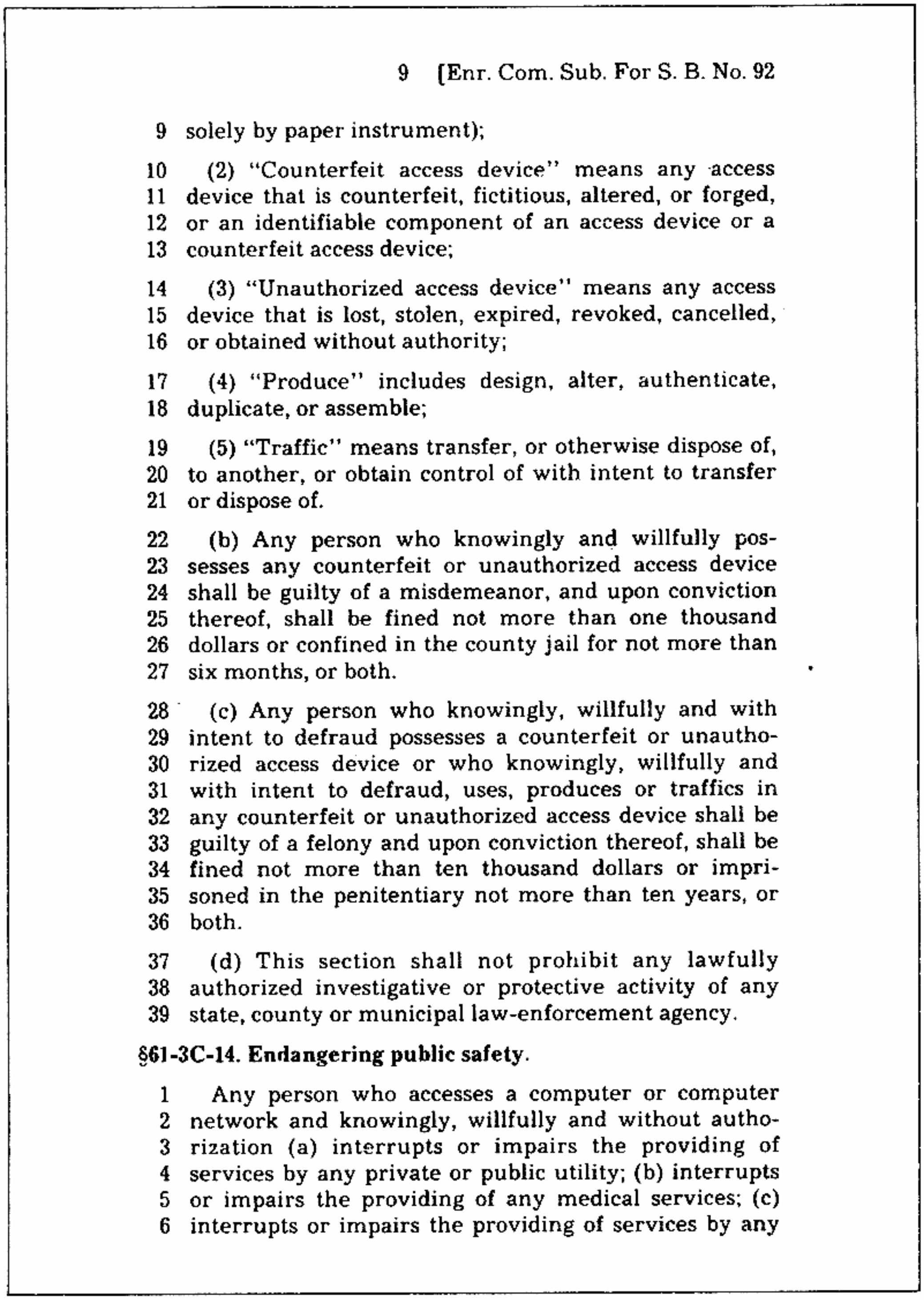
§61-3C-12. Computer invasion of privacy.

Any person who knowingly, willfully and without authorization, accesses a computer or computer network and examines any employment, salary, credit or any other financial or personal information relating to any other person, after the time at which the offender knows or reasonably should know that he is without authorization to view the information displayed, shall be guilty of a misdemeanor, and upon conviction thereof, shall be fined not more than five hundred dollars, or confined in the county jail for not more than six months, or both.

§61-3C-13. Fraud and related activity in connection with access devices.

(a) As used in this section, the following terms shall have the following meanings:

(1) "Access device" means any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated



solely by paper instrument);

(2) "Counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) "Unauthorized access device" means any access device that is lost, stolen, expired, revoked, cancelled, or obtained without authority;

(4) "Produce" includes design, alter, authenticate, duplicate, or assemble;

(5) "Traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of.

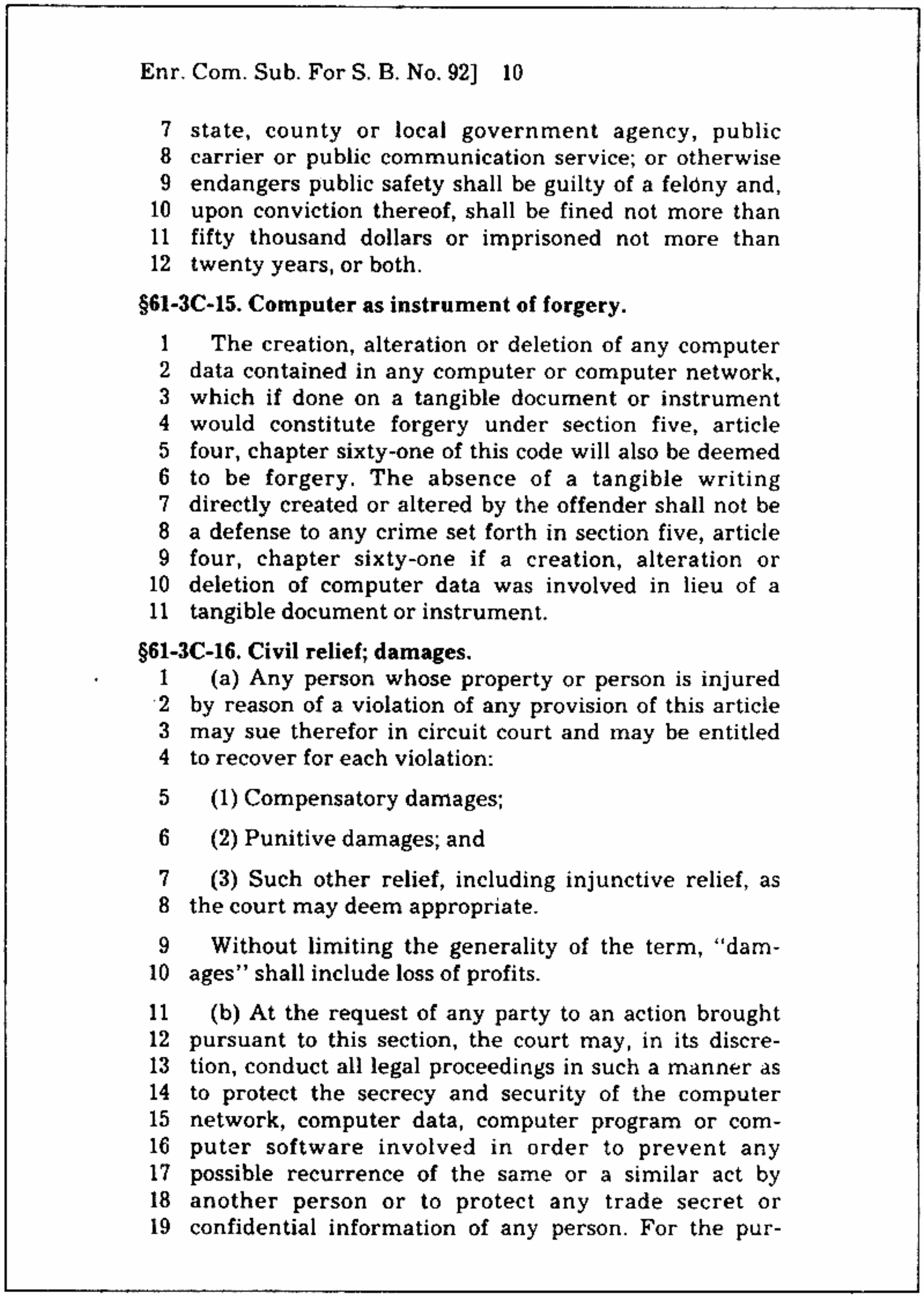
(b) Any person who knowingly and willfully possesses any counterfeit or unauthorized access device shall be guilty of a misdemeanor, and upon conviction thereof, shall be fined not more than one thousand dollars or confined in the county jail for not more than six months, or both.

(c) Any person who knowingly, willfully and with intent to defraud possesses a counterfeit or unauthorized access device or who knowingly, willfully and with intent to defraud, uses, produces or traffics in any counterfeit or unauthorized access device shall be guilty of a felony and upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary not more than ten years, or both.

(d) This section shall not prohibit any lawfully authorized investigative or protective activity of any state, county or municipal law-enforcement agency.

§61-3C-14. Endangering public safety.

Any person who accesses a computer or computer network and knowingly, willfully and without authorization (a) interrupts or impairs the providing of services by any private or public utility; (b) interrupts or impairs the providing of any medical services; (c) interrupts or impairs the providing of services by any



state, county or local government agency, public carrier or public communication service; or otherwise endangers public safety shall be guilty of a felony and, upon conviction thereof, shall be fined not more than fifty thousand dollars or imprisoned not more than twenty years, or both.

§61-3C-15. Computer as instrument of forgery.

The creation, alteration or deletion of any computer data contained in any computer or computer network, which if done on a tangible document or instrument would constitute forgery under section five, article four, chapter sixty-one of this code will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any crime set forth in section five, article four, chapter sixty-one if a creation, alteration or deletion of computer data was involved in lieu of a tangible document or instrument.

§61-3C-16. Civil relief; damages.

(a) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor in circuit court and may be entitled to recover for each violation:

(1) Compensatory damages;

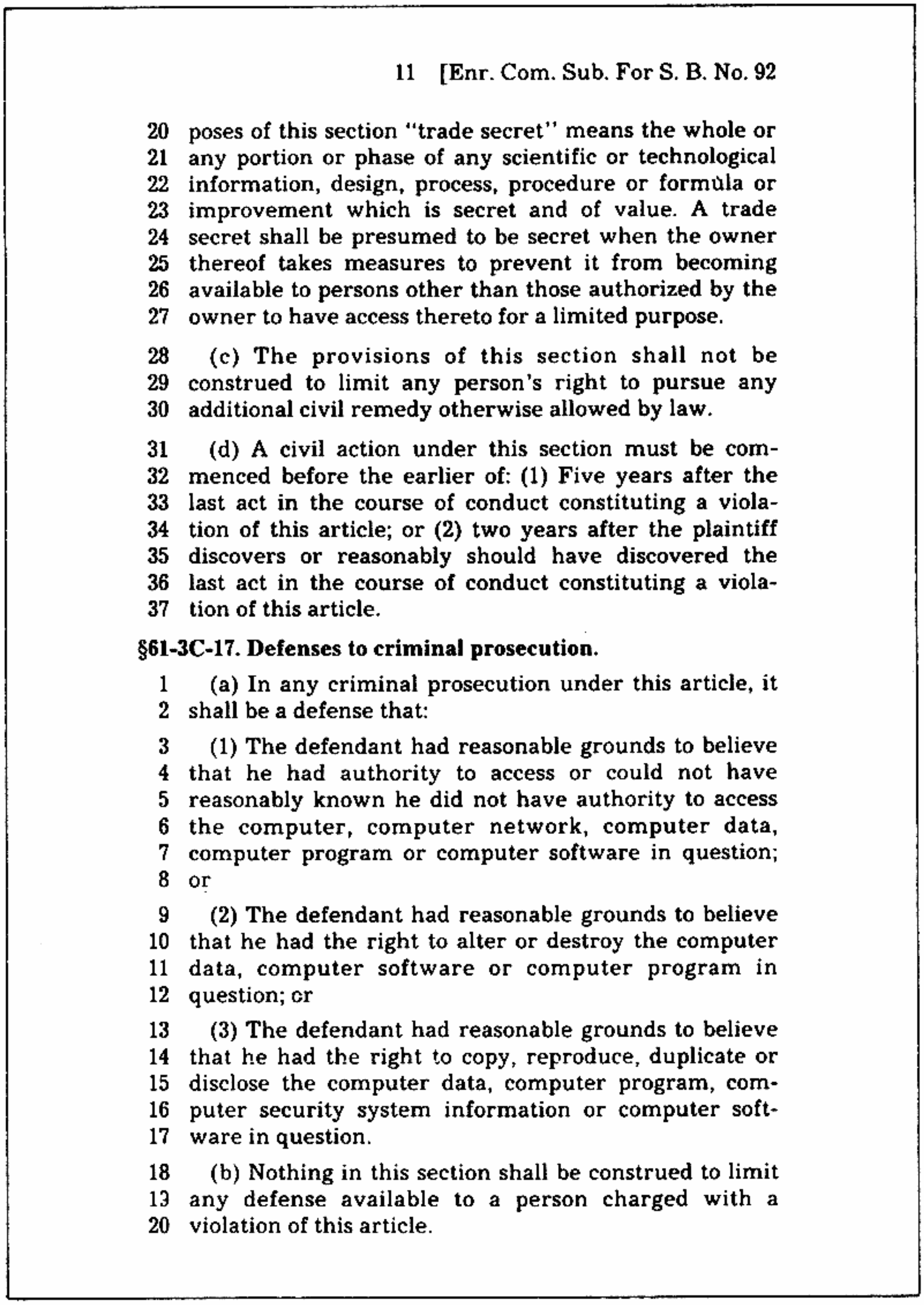
(2) Punitive damages; and

(3) Such other relief, including injunctive relief, as the court may deem appropriate.

Without limiting the generality of the term, "damages" shall include loss of profits.

(b) At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a manner as to protect the secrecy and security of the computer network, computer data, computer program or computer software involved in order to prevent any possible recurrence of the same or a similar act by another person or to protect any trade secret or confidential information of any person. For the pur-

Appendix F (continued)



poses of this section "trade secret" means the whole or any portion or phase of any scientific or technological information, design, process, procedure or formula or improvement which is secret and of value. A trade secret shall be presumed to be secret when the owner thereof takes measures to prevent it from becoming available to persons other than those authorized by the owner to have access thereto for a limited purpose.

(c) The provisions of this section shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(d) A civil action under this section must be commenced before the earlier of: (1) Five years after the last act in the course of conduct constituting a violation of this article; or (2) two years after the plaintiff discovers or reasonably should have discovered the last act in the course of conduct constituting a violation of this article.

§61-3C-17. Defenses to criminal prosecution.

(a) In any criminal prosecution under this article, it shall be a defense that:

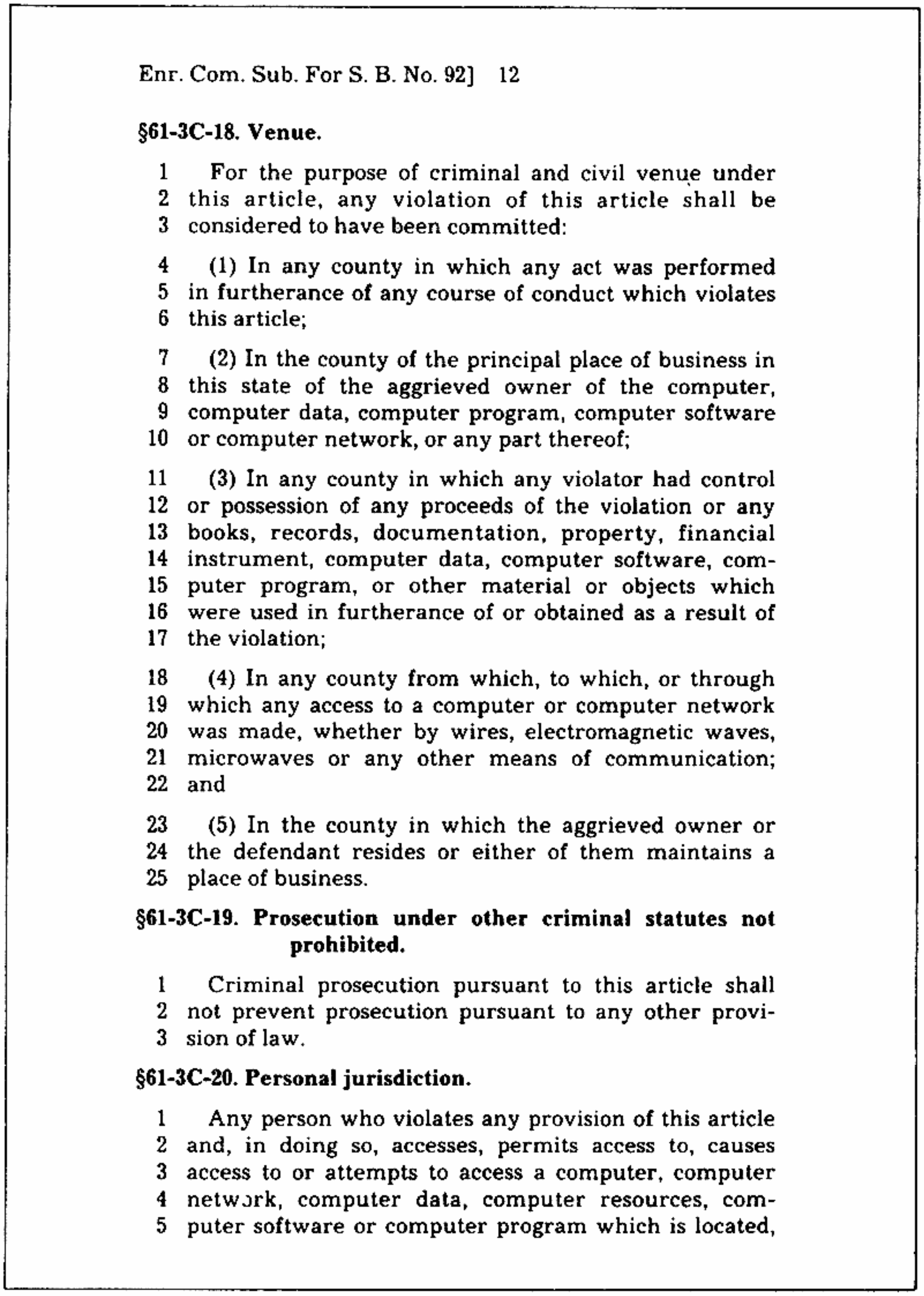
(1) The defendant had reasonable grounds to believe that he had authority to access or could not have reasonably known he did not have authority to access the computer, computer network, computer data, computer program or computer software in question; or

(2) The defendant had reasonable grounds to believe that he had the right to alter or destroy the computer data, computer software or computer program in question; cr

(3) The defendant had reasonable grounds to believe that he had the right to copy, reproduce, duplicate or disclose the computer data, computer program, computer security system information or computer software in question.

(b) Nothing in this section shall be construed to limit any defense available to a person charged with a violation of this article.

Appendix F (continued)



§61-3C-18. Venue.

For the purpose of criminal and civil venue under this article, any violation of this article shall be considered to have been committed:

(1) In any county in which any act was performed in furtherance of any course of conduct which violates this article;

(2) In the county of the principal place of business in this state of the aggrieved owner of the computer, computer data, computer program, computer software or computer network, or any part thereof;

(3) In any county in which any violator had control or possession of any proceeds of the violation or any books, records, documentation, property, financial instrument, computer data, computer software, computer program, or other material or objects which were used in furtherance of or obtained as a result of the violation;

(4) In any county from which, to which, or through which any access to a computer or computer network was made, whether by wires, electromagnetic waves, microwaves or any other means of communication; and

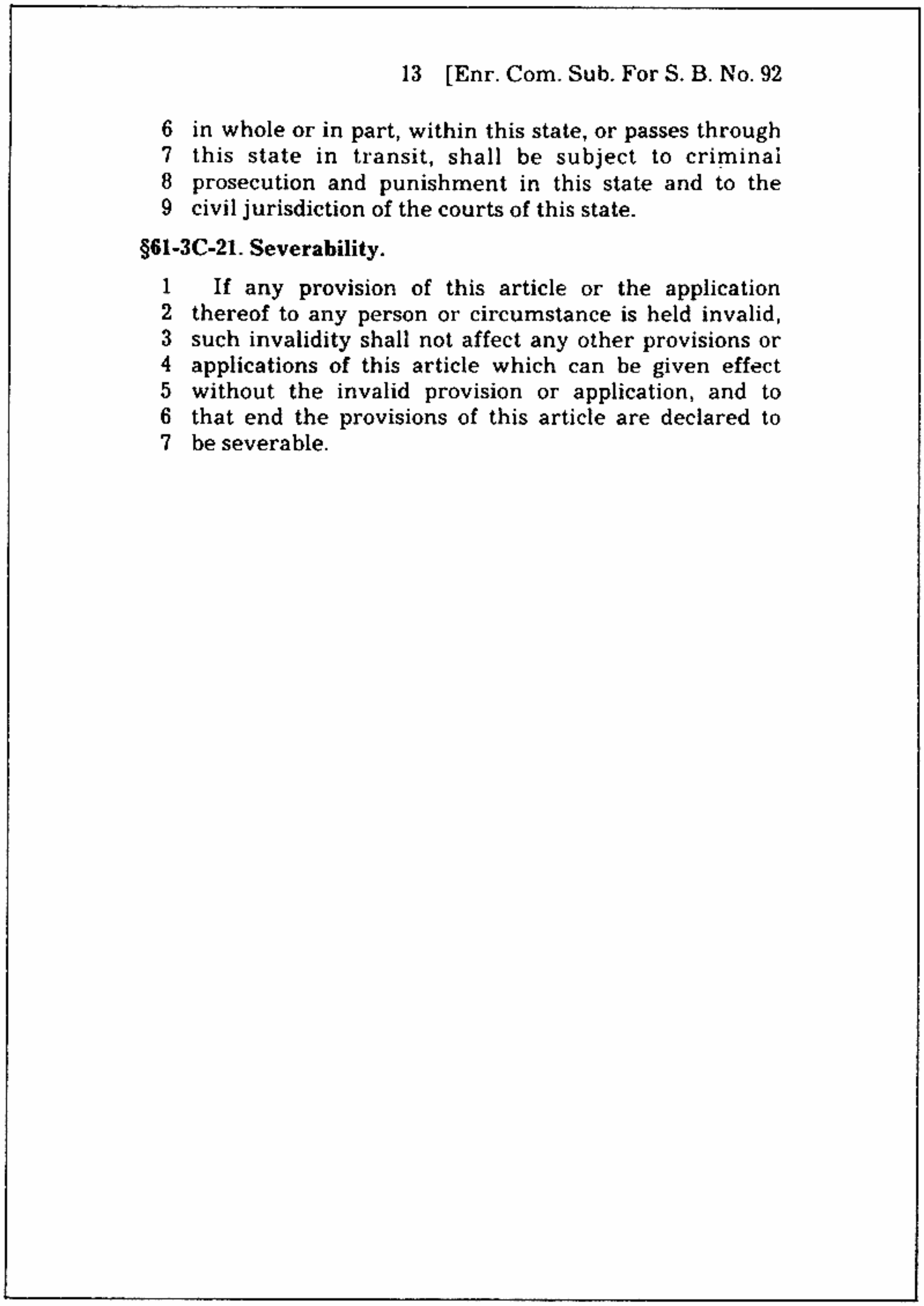
(5) In the county in which the aggrieved owner or the defendant resides or either of them maintains a place of business.

§61-3C-19. Prosecution under other criminal statutes not prohibited.

Criminal prosecution pursuant to this article shall not prevent prosecution pursuant to any other provision of law.

§61-3C-20. Personal jurisdiction.

Any person who violates any provision of this article and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources, computer software or computer program which is located,



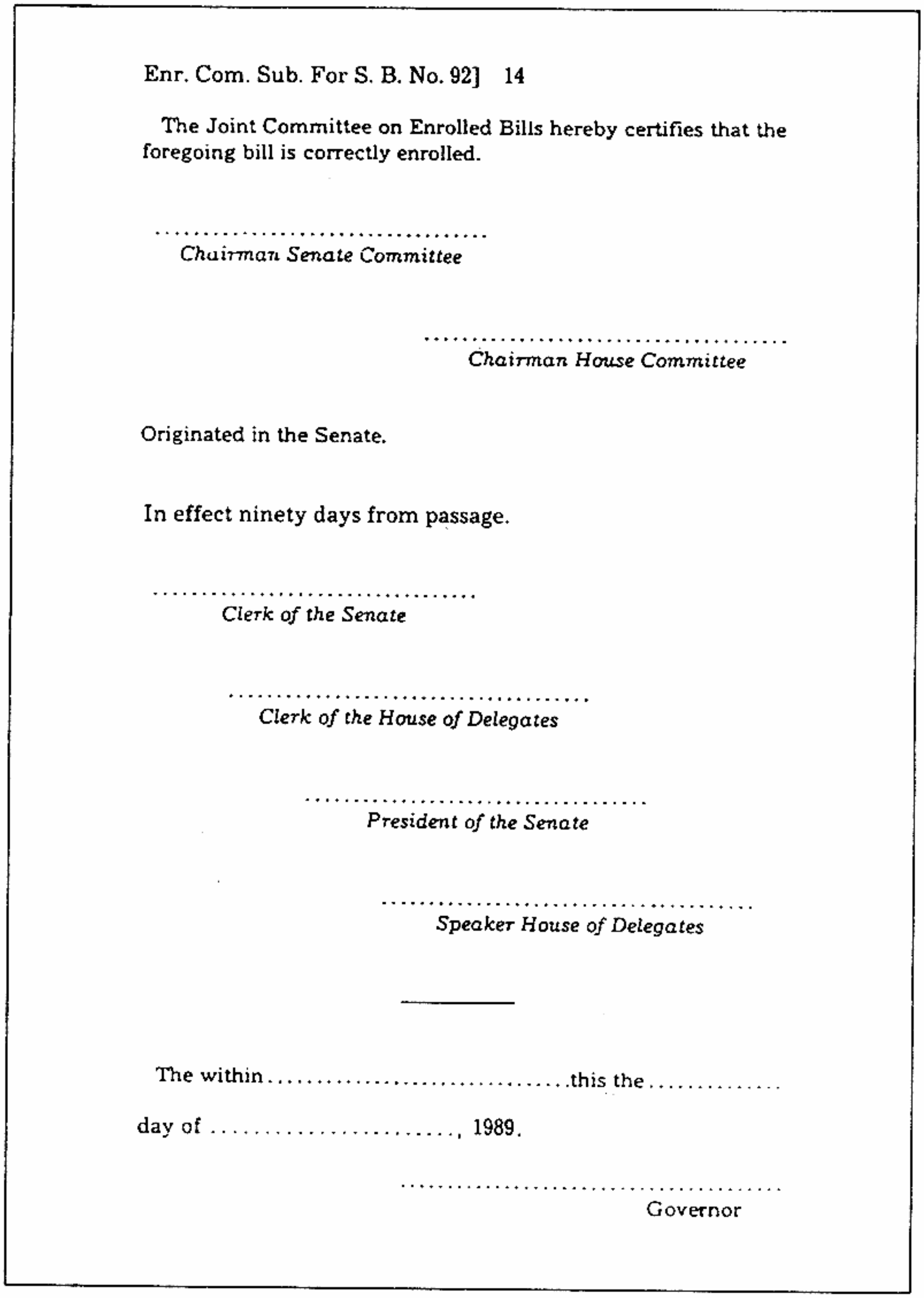
13 [Enr. Com. Sub. For S. B. No. 92

in whole or in part, within this state, or passes through this state in transit, shall be subject to criminal prosecution and punishment in this state and to the civil jurisdiction of the courts of this state.

§61-3C-21. Severability.

If any provision of this article or the application thereof to any person or circumstance is held invalid, such invalidity shall not affect any other provisions or applications of this article which can be given effect without the invalid provision or application, and to that end the provisions of this article are declared to be severable.

Appendix F (continued)



Enr. Com. Sub. For S. B. No. 92] 14

The Joint Committee on Enrolled Bills hereby certifies that the foregoing bill is correctly enrolled.

....
Chairman Senate Committee

....
Chairman House Committee

Originated in the Senate.

In effect ninety days from passage.

....
Clerk of the Senate

....
Clerk of the House of Delegates

....
President of the Senate

....
Speaker House of Delegates

The within ....this the ....

day of ...., 1989.

....
Governor

REFERENCES

[1] Alexander, Michael, "FBI expected to throw book at virus suspect", COMPUTERWORLD, February 6, 1989, p.2.

[2] ANON, "British Computer Users Have an Unlucky 13th", THE NEW YORK TIMES, January 14, 1989, s.1,p.5,c.3.

[3] ____, "Computer hacker indicted:, UPI, December 20, 1988, BC Cycle, NEXIS.

[3a] ____, "Computer Hacking Suspect a Legend to Some; A Threat to Others", AP, June 3, 1989, NEXIS.

[3b] ____, "Computer Virus Creator Indicted," WASHINGTON POST, July 27, 1989, p. A-20.

[4] ____, "Disruptive File Distributed Through IBM Systems, December 14, 1987, 12/16 a.m., IBM Internal Memo.

[4a] ____, "Drop the Phone; Busting a Computer Whiz", TIME, January 9, 1989, p.49.

[5] _____, "Empirical Research Systems Inc. files patent on hardware/software solution to computer virus", BUSINESS WIRE, May 10, 1989, NEXIS.

[6] ____, "Friends say Student tried to halt 'virus', BOSTON GLOBE, November 7, 1988, p.3

[7] ____, "Hot Bills for '89", COMPUTERWORLD, December 16, 1989, p.12.

[8] ____, "Indifference Opened Door to Computer Virus", LOS ANGELES TIMES, November 12, 1988, p.1.

[9] ____, "Insurance May Cover Computer Virus Losses: Corroon & Black", PR Newswire, May 24, 1989, NEXIS.

[10] ____, "Meeting the Threat", THE AMERICAN BANKER, February 2, 1989, p.8.

[11] ____, "Microkid Raids", TIME, October 24, 1983, p,59.

[12] ____, "Minnesota Legislative Briefs", UPI, April 28, 1989, BC Cycle, NEXIS.

[12a] ____, "Pentagon 'Swat Team' for Computer Hackers", UPI, December 6, 1988, NEXIS.

[13] ____, "Purdue Agrees to Withhold Details of Computer Virus", LOS ANGELES TIMES, November 12, 1988, p.27.

[14] ____, "Researchers Fear Computer 'Virus' Will Slow Use of National Network", NEW YORK TIMES, November 14, 1988, p.B6, c1.

[15] ____, "Steal the Lock First", BOSTON GLOBE, January 31, 1989, p.39.

[16] ____, "The Kid Put us Out of Action", TIME, November 14, 1988, p.76.

[17] ____, "The Nation; Pentagon Plans Computer 'Virus' Team", LA TIMES, December 7, 1988, part 1, p.2, c.3.

[18] ____, "The Viral Vanguard", BOSTON GLOBE, March 7, 1989,p.59.

[19] ____, "Virus Cleanup: About $96 million", USA TODAY, November 17, 1988, p.4b.

[20] Anthes, Gary H., "Task Forces Work to Keep INTERNET Safer", FEDERAL COMPUTER WEEK, November 14, 1988. p.1.

[21] Arnst, Catherine, "Computer Viruses Spawn Anti-Viral Industry", THE REUTER LIBRARY REPORT, December 7, 1988, NEXIS.

[22] Barr, Cameron, "Antiviral Agent Foils Computer Bugs", THE AMERICAN LAWYER, November 1988, p.116.

[23] Becket, Michael, "The Game's Up for Hackers", THE DAILY TELEGRAPH, May 22, 1989, p.27.

[24] Bigelow, Robert, "Computer Security, Crime and Privacy --- U.S. Status Report", 6 THE COMPUTER LAW AND SECURITY REPORT 10, March-April 1989.

[25] ________, "Computer Security Crime and Privacy", THE COMPUTER LAWYER, v. 6, no. 2, February 1989, p.10.

[26] BloomBecker, J.J. Buck, "Cracking Down on Computer Crime" LEGISLATURES, August 1988, p.10.

[27] ___________, "Can computer crime laws stop spread of viruses?", COMPUTER LAW STRATEGIST, v.V, no. 10, February 1989, p.1. A check of proposed legislation was also conducted by Ronald Palenski for Adapso and provided to the author by letter dated July 10, 1989.

[28] Burger, Ralf, COMPUTER VIRUSES: A HIGH TECH DISEASE, Grand Rapids, MI: Abacus 1988).

[29] Chandler, David L., "No system immune from 'virus' attack", BOSTON GLOBE, December 4, 1988, BOSTON GLOBE, p.1.

[30] Clancy, Heather, "Panel: Training and Standards Needed for Computer Security", UPI, April 26, 1989, NEXIS.

[31] Coale, Kristi, "Razor Blades in Apples...", MAC USER, September 1988, NEXIS.

[32] David, John, "Treating Viral Fever", COMPUTERS & SECURITY, v. 7, no. 3, June 1988, p.255.

[33] Davidson, Stephen, Minnesota Bar Association Computer Law Section, Interview, May 22, 1989.

[34] Denning, Peter J., "Computer Viruses", 76 AMERICAN SCIENTIST 236, May-June 1988.

[35] Deutsch, Linda, "Government Strikes Plea Bargain with 'Dangerous' Hacker", AP, March 16, 1989, PM Cycle, NEXIS.

[35a] Dewdney, A. K., "Of worms, viruses and Core War, Computer Recreations", SCIENTIFIC AMERICAN, v. 260, p. 110, March 1989.

[35b] _______, "In the game called Core War hostile programs engage in a battle of bits: Mathematical recreations", SCIENTIFIC AMERICAN, v. 250, p. 14, May 1984.

[35c] _______, "A Core War bestiary of viruses, worms and other threats to computer memories", SCIENTIFIC AMERICAN, v. 252, p. 14, March 1985.

[36] Di Dio, Laura, "A menace to society; Increasingly sophisticated -- and destructive -- computer viruses may begin to take their toll in lives as well as dollars", NETWORK WORLD, February 6, 1989, p.71.

[37] ________, "Local Networking", NETWORK, WORLD, January 23, 1989, p.23.

[38] Diffie, Whitfield, Bell-Northern Research, Telephone Interview, May 16, 1989.

[39] Dolinar, "Preventive Medicine for Computer Virus", NEWSDAY, April 4, 1989, p.20.

[40] Doyle, T.C., "Microbe-computer? Industry Struggles for 'Virus' Vaccine, 6 COMPUTER & SOFTWARE NEWS 23, June 6, 1988, p.1.

[41] Elmer-DeWitt, Philip, "Invasion of the Data Snatchers", TIME, September 26, 1988, p.62.

[42] Esposito, Richard, "Computer as a Weapon: L.A. Hacker Charged", NEWSDAY, December 17, 1988.

[43] Farkas, Brian, "Computer crimes act endorsed", UPI, March 30, 1989, BC cycle.

[44] Feldman, Paul, "Prosecutors Seek Tough 'Virus Laws', LA TIMES, December 19, 1988, F24.

[44a] Feynmen, Richard P., "Safecracker Suite: Drumming and Storytelling," Compact Disc, Ralph Leighton, Box 70021, Pasadena, CA 91107, 1988.

[45] ______, SURELY YOU'RE JOKING MR. FEYNMAN, ADVENTURES OF A CURIOUS CHARACTER (New York: W.W. Norton, 1985).

[46] Friis, M. William, "Is Your PC Infected?", ABA BANKING JOURNAL, American Bar Association, May 1989, p.49.

[47] Gewartz, Catherine, "Computer hacker pleads innocent to telephone charge", UPI, February 3, 1989, NEXIS.

[47a] Gemignani, Michael, "Viruses and Criminal Law", Communications of the ACM. Vol. 32, no.6, p.669, June 1989.

[48] Gillette, Robert, "Computers Stumped by Ethics Code" LOS ANGELES TIMES, November 12, 1988, p.1.

[49] Gordon, Al, "Conviction in Computer 'Time Bomb'", NEWSDAY, September 21, 1988, p.41.

[50] Gordon, Gregory, "Tighter Computer Security Urged", UPI, May 16, 1989, NEXIS.

[51] Griffiths, Lyndsay, "Contagious Computer Virus Infects Hundreds of Machines", REUTER BUSINESS REPORT, January 13, 1989, BC cycle, NEXIS.

[52] Guidobono, Thomas, Defense Attorney for RTM, Telephone Interview, April 11, 1989.

[53] Hafner, K. et al., "Is Your Computer Secure?", BUSINESS WEEK, August 1, 1988, cover story, p.64.

[53a] Hanson, C., "Computer Virus is Threat to Key Defense, Banking Systems", REUTER BUSINESS REPORT, August 4, 1986, via NEXIS.

[54] Harber, Aaron, "For Robert T. Morris, Jr., hacker, there's no excuse", BOSTON GLOBE, December 13, 1988, p.50.

[55] Helfant, R., and McLoughlin, G.J., "Computer Viruses: Technical Overview and Policy Considerations", Congressional Research Service, Library of Congress, December 15, 1988.

[56] Highland, Esther, " Cornell ARAPANET/MILNET Virus", COMPUTERS & SECURITY, February 1989, v.8. no.1, p.4.

[57] Highland, Harold, "The Scourge of Computer Viruses", SCIENCE, April 8, 1988. p.133.

[58] _______, "Computer Viruses and Sudden Death", vol. 6 No. 1, COMPUTERS & SECURITY, February 1987, p.8.

[59] _______, "The Brain Virus: Fact and Fancy", COMPUTERS & SECURITY, v. 7. no. 4, August 1988, p.367.

[60] Hiscock, John, "Hacker faces 'electronic terror' charge", THE DAILY TELEGRAM, January 10, 1989, p.8.

[61] Joint Legislative Budget and Finance Committee, Pennsylvania State Legislature, "Study of Computer Viruses and their Potential for Infecting Commonwealth Computer Systems," September 1988.

[62] Johnson, John, "Computer an 'Umbilical Cord to his Soul'; 'Dark Side' Hacker Seen as 'Electronic Terrorist'", LA TIMES, January 8, 1989, part 1,p.1,c.1.

[63] Johnson, Stuart J., "Computer Virus Spreads to Commercial Software", INFOWORLD, March 21, 1988, p.85.

[64] Joyce, Edward J., "Inside the Texas Virus Trial:, COMPUTER & COMMUNICATIONS DECISIONS (Information Access Company, 1989) via NEXIS.

[65] Kahn, Phyllis L., Proposed Study of State Computer Crime Laws, 1988.

[66] Kaplan, Fred, "FBI 'virus' probe moves to Cornell", BOSTON GLOBE, November 9, 1988, p.14.

[67] ________, "Pentagon says systems are secure; others insist no defense is perfect", BOSTON GLOBE, December 5, 1988, p.1.

[68] Kluth, Daniel J., "The Computer Virus Threat or The Need to Amend Minnesota's Computer Crime Statutes", 6 MINNESOTA STATE BAR ASSOCIATION COMPUTER LAW SECTION NEWS NO. 3, Spring 1989.

[69] Korn, Carl, "Tougher penalties urged for computer hackers", UPI, March 8, 1989, BC cycle, NEXIS.

[70] Levy, Steven, HACKERS: HEROES OF THE COMPUTER REVOLUTION (Garden City, NY: Doubleday, 1984).

[71] Lynn, M. Stuart, Commission Chair, et al, THE WORM: A REPORT TO THE PROVOST OF CORNELL UNIVERSITY AND AN INVESTIGATION CONDUCTED BY THE COMMISSION OF PRELIMINARY ENQUIRY, Cornell University, February 6, 1989. Reprinted in COMMUNICATIONS OF THE ACM, vol.32, no. 6, p. 706, June 1989.

[72] Markoff, John, "Californian Held in Computer Case", NEW YORK TIMES, December 26, 1988, s.1, p.13, c.1.

[73] _______, "Cyberpunks Seek Thrills In Computerized Mischief", NEW YORK TIMES NEWS SERVICE, November 26, 1988, NEXIS.

[74] _______, "Innocent Experiment Went Awry", SUNDAY TENNESSEAN, November 6, 1988, p.8-A.

[74a] _______, "Student, After Delay, Is Charged in Crippling of Computer Network," NEW YORK TIMES, July 27, 1989.

[75] ________, "Virus Outbreaks Thwart Computer Experts", NEW YORK TIMES, May 30, 1989, p.C1.

[76] Marshall, Eliot, "Worm Invades Computer Networks", SCIENCE, November 11, 1988, p.855.

[77] Maugh, Thomas. H. II, "Indifference Opened Door to Computer Virus", LOS ANGELES TIMES, November 12, 1988, p.1.

[78] McAfee, John, "The Six Most Common Computer Viruses", Unpublished Manuscript, 1988.

[78a] McLellan, V., "Computer Systems Under Siege", NEW YORK TIMES, B1, January 31, 1988.

[79] McCown, Davis, "The State of Texas v. Donald Gene Burleson: Case History and Summary of Testimony", September 1988, Tarrant County District Attorney's Office, Texas.

[80] _______, Telephone Interview, April 11, 1989.

[81] Millership, Peter, "Computer Open New Windows for Crime and Sabotage, REUTERS, February 16, 1989, BC cycle, NEXIS.

[82] Mitchell, Charles, "Soviet computers hit by virus", UPI, December 18, 1988, BC cycle, NEXIS.

[83] Murphy, Kim, "Computer Whiz Admits Criminal Mischief", LA TIMES, March 16, 1989, part 2, p.3, c.1.

[84] ______, "Judge Rejects Hacker's Plea Bargain", LA TIMES, April 25, 1989, part 2, p.31, c.3.

[85] Nelson, Robin, "Viruses, pests, and politics: state of the art", COMPUTER & COMMUNICATIONS DECISIONS, December 1988, Vol. 20, No. 12, p.40.

[85a] Palenski, Ronald, General Counsel of ADAPSO, by letter to author dated July 10, 1989.

[86] Peterzell, Jay. "Spying and Sabotage by Computer", TIME, March 20, 1989, p.25.

[87] Radai, Y, "PC-DOS-MS-DOS Viruses", DOCKMASTER, May 16, 1989.

[88] Rasch, Mark, U.S. Department of Justice, Telephone Interview, April 21, 1989 [writing a report on computer viruses for DOJ to be issued in summer 1989].

[89] Rebello, Kathy, "'Sensitive kid' faces fraud trial", USA TODAY, February 28, 1989, p.B-1.

[89a] Rheingold, H., "Computer viruses", WHOLE EARTH REVIEW, no. 60, p. 106, September 22, 1988.

[90] Richards, Evelyn, "Viruses Pull Computer Underground into Spotlight", THE WASHINGTON POST, February 5, 1989, H1.

[90a] Rochlis, J.A. and Eichin, Mark W., "With Microscope and Tweezers: The Worm from MIT's Perspective", COMMUNICATIONS OF THE ACM, Vol.32, no. 6, p. 689, June 1989.

[91] Rosenberg, Ronald, "System sabotage: A matter of time", BOSTON GLOBE, December 6, 1988, p.1.

[92] Rubenking, Neil J., "Infection Protection", PC, Vol.8, no.8, April 25, 1989, p.193.

[93] Samuelson, Pamela, "Computer Virus May Find Hole in the Law", THE ATLANTA JOURNAL, November 20, 1988, p.B1.

__________, "Can Hackers be sued for Damages Caused by Computer Viruses?", COMMUNICATION OF THE ACM, Vol. 32, no. 6, p. 666, June 1989.

[94] Savage, J.A., "Hacker pleads guilty to computer violations, is denied bail by judge", COMPUTERWORLD, March 20, 1989, p.16.

[95] ______, "Hacker prosecution; Suspect held, denied phone access by district court" COMPUTERWORLD, January 9, 1989, p.2.

[96] Schares, Gail, "A German Hackers' Club That Promotes Creative Chaos", BUSINESS WEEK, August 1, 1988, p.71.

[96a] Schuyten, P. J., "New Programs for Data Grids", NEW YORK TIMES, p. D2, November 13, 1980.

[97] Seeley, Donn, "A Tour of the Worm", Department of Computer Science, University of Utah. Reprinted in COMMUNICATIONS OF THE ACM, vol. 32, no. 6, p. 700, June 1989.

[97a] Shoch, J. F. and Hupp, J. H., "The 'Worm' Programs - Early Experience with a Distributed Computation", COMMUNICATIONS OF THE ACM, vol. 25, no. 3, p. 172, March 1982.

[98] Sims, Calvin, "Researchers Fear Computer Virus Will Slow Use of National Network", NEW YORK TIMES, November 14, p.B6.

[99] Software Development Council, "Developer's Virus Task Force", January 20, 1989.

[100] Solomon, R. J., and Anania, L. "The Vulnerability of the Computerized Society", TELECOMMUNICATIONS, April 1987, p.30.

[101] Spafford, Eugene H., "The INTERNET Worm Program: An Analysis", PURDUE TECHNICAL REPORT CSD-TR-823, Revision December 1988. Reprinted in COMMUNICATIONS OF THE ACM, vol. 32, no. 6, p. 678, June 1989.

[102] Stallman, Richard M., "Why Software Ownership is bad for Society", Talk given at University of Texas, February 1987.

[103] Stoll, Cliff, "How Secure are Computers in the USA? An Analysis of a Series of Attacks on Milnet Computers", COMPUTERS & SECURITY, v. 7. no. 6, December 1988, p.543.

[104] _____, "Stalking the Wily Hacker", COMMUNICATIONS OF THE ACM, v. 31, no. 5, May 1988, p.485.

[105] _____, Personal Interview, April 19, 1989.

[106] Tibbits, George, "Commercial Software Discovered in New Aldus Program", AP, March 16, 1988, PM cycle, NEXIS.

[107] Van, Jon, "Oddballs no more, hackers are now threat", CHICAGO TRIBUNE, March 5, 1989, Perspective, p.4.

[108] Various authors: "Special Symposium, Computer Viruses", COMPUTERS & SECURITY, v.7, no.2, April 1988.

[109] Waldorf, M & May, J., "Virus Hits the INTERNET", HARVARD COMPUTER REVIEW, November 1988, p.8.

[110] Waldrop, M. Mitchell, "Parc Brings Adam Smith to Computing", 244 SCIENCE 145, April 14, 1989.

[111] Wines, Michael, "A Family's Passion for Computers, Gone Sour", NEW YORK TIMES, p.1.

[112] Young, Cliff, "Virus Epidemic", HARVARD COMPUTER REVIEW, November 1988, p.4.

[113] Zajac, Bernard P., Jr., "Legal• Options to Computer Viruses", COMPUTERS & SECURITY, v.8, no.1, February 1989, p.25.

[114] _____, "Viruses: Should We Quit Talking About Them?" COMPUTERS & SECURITY, v.7 no.5, October 1988, p.471.

[115] "TRAP DOOR" - A re-entry point left in a computer's otherwise secure operating system by the designer, allegedly to permit a programmer with knowledge of it to re-enter and to correct errors or to improve performance. The invasion of the INTERNET worm was said to be facilitated by the discovery by RTM of a "trap door" in the Berkeley version of UNIX. Many software programmers favor "trap doors" as facilitating the improvement of performance by users. Some programmers criticize RTM for using what was a well-known "trap door" in the Berkeley UNIX 4.3 software package. Thus they characterize what RTM did not as an accomplishment but as an exercise in stupidity. [101] One

student said he would be embarrassed if he had written RTM's code. [76] The Cornell Report concludes that the code could have been written by any reasonably competent computer science student. [71] What remains unclear is whether standards of network integrity should preclude the existence of "trap doors" or any other weaknesses in access control. Thus an action in tort would require a determination of how "the rational computer programmer" would behave, thereby exposing a weakness in generally recognized ethical values and operating procedures.

[116] A federal grand jury in Syracuse, New York, indicted young Morris, on July 26, 1989, for gaining access to federal interest computers, preventing authorized access by others, and causing in excess of $1000 in damage. The computers alleged to have been affected were operated by NASA Ames Research Center, Wright Patterson Air Force Base, the University of California at Berkeley, and Purdue University. [74a, 3b]

[117] The indictment cited only 18 U.S.C. 1030(a)(5). U.S. v. Robert Tappan Morris, Case No. 89-CR-139, July 26, 1989.