

Before the
UNITED STATES SENTENCING COMMISSION
One Columbus Circle, N.E., Suite 2-500
Washington DC 20002-8002
Attention: Public Information

-----X

In the Matter of

Proposed Amendment of the Sentencing
Guidelines for the United States, Section
2F2.1, Applicable to Violations of the
Computer Fraud and Abuse Act

-----X

TO: The Commission

COMMENTS OF THE SOCIETY FOR ELECTRONIC ACCESS

The Society for Electronic Access ("SEA") submits these comments in the above-captioned proceeding, which concerns the proposed amendments to the United States Sentencing Guidelines ("U.S.S.G.") concerning Computer Fraud and Abuse [57 Fed. Reg. 62832 (1992) (to be codified at U.S.S.G. sec. 2F2.1) (proposed Dec. 31, 1992)]. We strongly urge you not to adopt these amendments because the penalties specified therein are unduly harsh, overly broad, and vague.

These amendments violate due process by providing harsher penalties for activities more properly related to computing than to crime. For example, proposed U.S.S.G. sec. 2F2.1.b.1 states:

"If the defendant altered information, increase by 2 levels"
where alteration is defined in Commentary #9 as including:

"...all changes to data, whether the defendant added, deleted, amended or destroyed any or all of it."

It is almost impossible to use a computer without performing one or more of these functions. Merely logging on to another

computer fits this definition of alteration because this changes the information kept in its system logs, even if the user never requested that a specific file or record be accessed.

Furthermore, the effect of these data alterations may not be directly related to severity of a crime: if a voyeur looks at protected files and leaves a note telling that he or she was there, that is very different from a vandal's deletion of a credit file. Yet, under these amendments both situations are treated as activities of equal seriousness. It is absurd to think that the alteration itself, absent other factors, requires an increase in the severity of the minimum sentence, or that all alterations affect criminality equally.

These amendments violate due process by including overly broad standards for determining the severity of a crime. For example, proposed U.S.S.G. sec. 2F2.1.b.5 states:

"If an offense was committed for the purpose of malicious destruction or damage, increase by 4 levels."

where malicious destruction or damage, as defined in Commentary #11:

". . . includes injury to business and personal reputations."

The effect of so broad a category of activity being contained in a single sentencing adjustment would be to group the trivial with the heinous, and punish them equally. Breaking into a person's computer account and publicly posting information which disrupts his or her ability to conduct business is very different matter

from copying and publicly posting materials from that person's account that simply make the person look foolish, yet the amendment groups these actions together as offenses of equal seriousness.

Furthermore, this language allows for the punishment of speech without requiring a determination that the speech does not enjoy the protection of the First Amendment. The Supreme Court has always erected extremely stringent standards for the kinds of speech that can be found unprotected by the First Amendment, and these amendments to the Sentencing Guidelines err by allowing speech to be punished if it is found to damage someone's "personal reputation" under less stringent standards of proof, which would be introduced at the sentencing, rather than at the trial itself.

These amendments violate due process by mandating overly harsh punishments. To use an example derived from the recent past (see Salinger v. Random House, 811 F.2d 90 (2d Cir.), cert. denied, 484 U.S. 890 (1987)), if a defendant (willfully and for the purposes of commercial advantage or private financial gain) wrote something for publication which included sections of J.D. Salinger's private correspondence, the defendant could be convicted of criminal copyright infringement, and fined. See 17 U.S.C. sec. 506 and 18 U.S.C. sec. 2319. It stretches the imagination, however, to suggest that if the defendant had either obtained or distributed these materials electronically, no matter how limited the scope of the distribution, this copyright

infringement would be transformed into a crime so severe that the defendant would, as a first time offender, face a sentence of fifteen to twenty-one (15-21) months in prison.

Proposed U.S.S.G. sec. 2F2.1.b.2 states:

"...if the defendant disclosed protected information to the public by means of a general distribution system, increase by six levels."

where the definition of "general distribution system" as defined in Commentary #10 includes:

"...electronic bulletin board and voice mail systems, newsletters and other publications, and any other form of group dissemination, by any means."

These amendments suggest that crimes for which the trial judge has heretofore had the latitude to impose probationary sentences or fines or both must now receive minimum sentences harsher than those mandated by the Federal Sentencing Guidelines for assault where the use of a dangerous weapon was threatened [U.S.S.G. sec. 2A2.3.a.1], sexual abuse of a ward [U.S.S.G. sec. 2A3.3.9.a] or trespassing on government property with a firearm [U.S.S.G. sec. 2B2.3.B.1 - .2]. Of all the potential violations of due process contained in these amendments, this potential for mandating unduly harsh sentences is the most shocking and the most clear.

In President Clinton's statement, "Technology for America's Economic Growth: A New Direction to Build Economic Strength" he says "Government telecommunication and information policy has not kept pace with new developments in telecommunications and computer technology. As a result, government regulations have

tended to inhibit competition and delay deployment of new technology." These amendments are part of that problem.

By simultaneously rendering the Guidelines both harsher and more vague, these amendments would create a chilling effect on perfectly legal uses of computers by private citizens, by creating an environment in which the potential criminality of an action would be impossible to ascertain in advance. Therefore, the SEA strongly urges you not to adopt the amendments to United States Sentencing Guidelines proposed at 57 Fed. Reg. 62832.

Respectfully submitted,



Society for Electronic Access
c/o Steven E. Barber
595 West End Avenue, Apt. 9D
New York, New York 10024
(212) 787-8421
sea@panix.com

Simona Nass, President
Alexis Rosen, Vice-President
Daniel Lieberman, Treasurer
Steven E. Barber, Secretary

Board of Directors:
Stacy Horn, Chair
Joseph King
John McMullen
Simona Nass
E. Lance Rose
Alexis Rosen
Paul Wallich

Date: March 15, 1993

Individual-Signers

Peter Bachman
145 State Street
Saratoga Springs, NY 12866
pbachman@skidmore.edu

Jim Baumbach
162 West 13 St.
NY, NY 10011
jsb@panix.com

Rod Bicknell,
3451 Giles Place, M-13,
Bronx, NY 10463,
76060.1255@compuserve.com

Eric Braun
691 Union Street
Brooklyn, New York 12215
gbs@panix.com

Steven Cherry
Manager
Publishing Technologies
Elsevier Science Publishing
Co., Inc.
9 E 16th St #3B
New York NY 10003
stc@panix.com

Mara Chibnik
875 West End Ave.
NY, NY 10025
mara@panix.com

Michael Cosaboom
Interactive Telecommunications
Program
New York University
441 1st Street #1R
Brooklyn, NY 11215
cosaboom@acf3.nyu.edu

Julian Dibbell
The Village Voice
476 Dean Street
Brooklyn NY 11217
718-636-8595
julian@panix.com

Andrew R. Funk
Chair, Radio Amateur
Telecommunications Society
14-23 31st Avenue Apt. 4A
Astoria, NY 11106-4559
kb7uv@panix.com

John Gilmore
Co-founder
Electronic Frontier Foundation
PO Box 170608
San Francisco, CA 94117
gnu@toad.com

Mike Godwin
Legal Services Counsel
Electronic Frontier Foundation
238 Main Steet, 4th Floor
Cambridge, MA 02142
617-576-4510
mnemonic@eff.org

John Hawkinson
1200 Warburton Ave, #57
Yonkers, NY 10701-1057
jhawk@panix.com

Brendan Kehoe
3364 Middlefield Road
Palo Alto, CA 94306
(415) 903 1400
brendan@lisa.cygnum.com

David S. Koosis
Director of Technical Services
Instructional Systems Company,
Inc.
14 East 4th Street, Suite 602
New York, NY 10012-1141
isc@panix.com

J.J. (Jean-Jacques) Larrea
Studson Soft Industries
144 West 17th Street 2RW
New York, NY 10011-5444
jjl@panix.com

Clay Shirky
33 Wooster Street
New York, NY 10013
clays@panix.com

Thor John Lancelot Simon
12 Elm Rock Road
Bronxville, NY 10708
(914) 779-7730
tls@panix.com

Sue Young
638 Washington Street #4B
New York NY 10014
(212) 243-6415
ysue@echo.panix.com



**Electronic Frontier
Foundation, Inc.**
666 Pennsylvania Avenue SE
Suite 303
Washington, DC 20003

Phone: (202)544-9237
Fax: (202)547-5481
Internet: jberman@eff.org

March 15, 1993

United States Sentencing Commission
One Columbus Circle, NE
Suite 2-500, South Lobby
Washington, DC 20002-9002
Attention: Public Information

Re: Proposed Amendent #59 to the Sentencing Guidelines for
United States Courts, which creates a new guideline applicable
to violations of the Computer Fraud and Abuse Act of 1988 (18
U.S.C. 1030)

Dear Commissioners:

The Electronic Frontier Foundation (EFF) writes to state our opposition to the new proposed sentencing guideline applicable to violations of the Computer Fraud and Abuse Act of 1988, 18 U.S.C. 1030 (CFAA). We believe that, while the proposed guideline promotes the Justice Department's interest in punishing those who engage in computer fraud and abuse, the guideline is much too harsh for first time offenders and those who perpetrate offenses under the statute without malice aforethought. In addition, promulgation of a sentencing guideline at the present time is premature, as there have been very few published opinions where judges have issued sentences for violations of the CFAA. Finally, in this developing area of the law, judges should be permitted to craft sentences that are just in relation to the facts of the specific cases before them.

The Proposed Guideline Is Too Harsh.

The proposed CFAA sentencing guideline, with a base offense level of six and innumerable enhancements, would impose strict felony liability for harms that computer users cause through sheer inadvertence. This guideline would require imprisonment for first time offenders who caused no real harm and meant none. EFF is opposed to computer trespass and theft, and we do not condone any unauthorized tampering with computers -- indeed, EFF's unequivocal belief is that the security of private computer systems and networks is both desirable and necessary to the maintenance of a free society. However, it is entirely contrary to our notions of justice to brand a computer user who did not intend to do harm as a felon. Under the proposed guideline, even a user who painstakingly attempts to avoid causing harm, but who causes harm nonetheless, will almost assuredly be required to serve some time in prison.

The proposed guideline, where the sentencing judge is given no discretion for crafting a just sentence based on the facts of the case, is too harsh on less culpable defendants, particularly first time offenders. As the Supreme Court has stated, the notion that a culpable mind is a necessary component of criminal guilt is "as universal and persistent in mature systems of law as belief in freedom of the human will and a consequent ability and duty of the normal individual to choose between good and evil." *Morrisette v. United States*, 342 U.S. 246, 250 (1952). In the words of another court, "[u]sually the stigma of criminal conviction is not visited upon citizens who are not morally to blame because they did not know they were doing wrong." *United States v. Marvin*, 687 F.2d 1221, 1226 (8th Cir. 1982), *cert. denied*, 460 U.S. 1081 (1983).

There Is Not Yet Enough Caselaw to Warrant a Guideline.

The Sentencing Commission itself has recognized the importance of drafting guidelines based on a large number of reported decisions. In the introduction to the Sentencing Commission's *Guidelines Manual*, the Commission states:

The Commission emphasizes that it drafted the initial guidelines with considerable caution. It examined the many hundreds of criminal statutes in the United States Code. It began with those that were the basis for a

significant number of prosecutions and sought to place them in a rational order. It developed additional distinctions relevant to the application of these provisions, and it applied sentencing ranges to each resulting category. In doing so, it relied upon pre-guidelines sentencing practice as revealed by its own statistical analyses based on summary reports of some 40,000 convictions, a sample of 10,000 augmented pre-sentence reports, the parole guidelines, and policy judgments.

United States Sentencing Commission, *Guidelines Manual*, Chap. 1, Part A (1991).

At the present time, there are only five reported decisions that mention the court's sentencing for violations of the Computer Fraud and Abuse Act. *See, United States v. Lewis*, 872 F.2d 1030 (6th Cir. 1989); *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), *cert. denied*, 112 S. Ct. 72 (1991); *United States v. Carron*, 1991 U.S. App. LEXIS 4838 (9th Cir. 1991); *United States v. Rice*, 1992 U.S. App. LEXIS 9562 (1992); and *United States v. DeMonte*, 1992 U.S. App. LEXIS 11392 (6th Cir. 1992). New communications technologies, in their earliest infancy, are becoming the subject of precedent-setting litigation. Overly strict sentences imposed for computer-related fraud and abuse may have the effect of chilling these technologies even as they develop. Five decisions are not enough on which to base a guideline to be used in such an important and growing area of the law.

The Commission itself has recognized that certain areas of federal criminal law and procedure are so new that policy statements, rather than inflexible guidelines, are preferable. *See, e.g., United States Sentencing Commission, Guidelines Manual*, Chap. 7, Part A (1990) (stating the Commission's choice to promulgate policy statements, rather than guidelines, for revocation of probation and supervised release "until federal judges, probation officers, practitioners, and others have the opportunity to evaluate and comment. . . ."). A flexible policy statement, rather than a specific sentencing guideline, is a more appropriate way to handle sentencing under the Computer Fraud and Abuse Act until there has been enough litigation on which to base a guideline.

Judges Must Be Permitted to Craft Their Own Sentences for Cases Involving Special Circumstances.

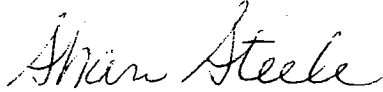
Individual sentencing decisions are best left to the discretion of the sentencing judge, who presumably is most familiar with the facts unique to each case. To promulgate an inflexible sentencing guideline, which would cover all crimes that could conceivably be prosecuted under the Computer Fraud and Abuse Act, is premature at this time.

As discussed above, there have only been five reported decisions where the Computer Fraud and Abuse Act has been applied. In three of these reported CFAA cases, the judges involved used their discretion and fashioned unique sentences for the defendants based on the special facts of the case. *See, Morris*, 928 F.2d at 506 (where the judge placed Defendant Morris on probation for three years to perform 400 hours of community service, ordered him to pay fines of \$10,050, and ordered him to pay for the cost of his supervision at a rate of \$91 a month); *Carron* at 3 (where the judge found that Defendant Carron's criminal history justified a sentence of 12 months incarceration followed by 12 months of supervised release and restitution to the two injured credit card companies); and *DeMonte* at 4 (where the trial court judge held that Defendant DeMonte's "extraordinary and unusual level of cooperation" warranted a sentence of three years probation with no incarceration). Judges must be permitted to continue fashioning sentencing that are just, based on the facts of a specific case.

Computer communications are still in their infancy. Legal precedents, particularly the application of a sentencing guideline to violations of the Computer Fraud and Abuse Act, can radically affect the course of the computer technology's future, and with it the fate of an important tool for the exchange of ideas in a democratic society. When the law limits or inhibits the use of new technologies, a grave injustice is being perpetrated. The Electronic Frontier Foundation respectfully asks the Commission to hold off promulgating a sentencing guideline for the Computer Fraud and Abuse Act until there are enough prosecutions on which to base a guideline.

Thank you in advance for your thoughtful consideration of our concerns. We would be pleased to provide the Commission with any further information that may be needed.

Sincerely yours,

A handwritten signature in cursive script that reads "Shari Steele". The signature is written in dark ink and is positioned above the printed name and title.

Shari Steele
Staff Attorney

The Electronic Frontier Foundation is a privately funded, tax-exempt, nonprofit organization concerned with the civil liberties, technical and social problems posed by the applications of new computing and telecommunications technology. Its founders include Mitchell Kapor, a leading pioneer in computer software development who founded the Lotus Development Corporation and developed the Lotus 1-2-3 Spreadsheet software.

CPSR

March 15, 1993

Chairman William W. Wilkins, Jr.
US Sentencing Commission
One Columbus Circle, NE
Suite 2-500
South Lobby
Washington, DC 20002-8002

Dear Mr. Chairman:

We are writing to you regarding the proposed amendments to sentencing guidelines, policy statements, and commentary announced in the Federal Register, December 31, 1992 (57 FR 63832). We are specifically interested in addressing proposed item 59, regarding the Computer Fraud and Abuse Act of 1988 (18 U.S.C. 1030).

CPSR is national membership organization of professionals in the computing field. We have a particular interest in information technology, including the protection of civil liberties and privacy. We have sponsored a number of public conferences to explore the issues involving computers, freedom, and privacy.¹

We have also testified before the House of Representatives and the Senate regarding the federal computer crime law.² It is our position that the government must be careful not to extend broad criminal sanctions to areas where technology is

¹ See, e.g., The First Conference on Computers, Freedom & Privacy (IEEE Computer Society Press 1991), The Second Conference on Computer, Freedom & Privacy (Association for Computing Machinery 1992). A third report will soon be out on the third Conference on Computers, Freedom & Privacy. All three volumes contain "reports from the field" that may be helpful in understanding more fully the issues related to the protection of computer systems, the conduct of computer crime investigations, and the appropriate penalties for computer crime.

² Computer Virus Legislation, Hearing before the Subcomm. on Criminal Justice, Comm. on the Judiciary, U.S. House of Rep., 101st Cong., 1st Sess. 62 (1989), The Computer Abuse Amendments Act of 1990, Hearing before the Subcomm. on Technology and the Law of the Comm. on the Judiciary, United States Senate, 101st Cong., 2d Sess. 62 (1990).

CPSR Washington Office
666 Pennsylvania Ave. S.E.
Suite 303
Washington, DC 20003
202 544-9240
Fax 202 547-5481/2
rotenberg@washofc.cpsr.org

Marc Rotenberg, Director
Richard Civile, Program Director
David Sobel, Staff Counsel

CPSR National Office
P.O. Box 717
Palo Alto, CA 94302
415 322-3778
Fax 415 322-3798
Nikki Draper, Office Manager
cpsr@csli.stanford.edu

CPSR Cambridge Office
P.O. Box 962
Cambridge, MA 02142
617 864-7329
Gary Chapman, Director
chapman@satfron.lcs.mit.edu

Advisory Board
Herbert L. Abrams
John Backus
Paul Brest
David Burnham
Dorothy Denning
Carol Edwards
Douglas Engelbart
Admiral Noel Gayler
Adele Goldberg
Richard Karp
Barbara Liskov
Elliot Maxwell
James Martin
Eli Noam
Karen Nussbaum
Severo M. Ornstein
Anthony Ralston
John Shattuck
Herbert Simon
Robert E. Tarjan
Robert W. Taylor
Lawrence Tesler
Sherry Turkle

Board of Directors

President
Eric Roberts

Chairperson
Jeff Johnson

Secretary
Todd Newman

Treasurer
Rodney Hoffman

Directors
Cathy Cook
Paul Hyland
Lesley Kalmin
Patti Lowe
Ivan Milman
Ronni Rosenberg
Douglas Schuler
Dan Williams
Terry Winograd
Coralee Whitcomb

rapidly evolving and terms are not well defined.³ We believe ~~that~~ such efforts, if not carefully considered, may ultimately jeopardize the use of new information technology to promote education, innovation, commerce, and public life.

We also remain concerned that criminal sanctions involving the use of information technologies may unnecessarily threaten important personal freedoms, such as speech, assembly, and privacy. It is the experience of the computing profession that misguided criminal investigation and the failure of law enforcement to fully understand the use of computer technology will have a detrimental impact on the entire community of computer users.

For example, you may wish to review the recent decision of Steve Jackson Games v. Secret Service,⁴ involving a challenge to the government's conduct of a particular computer crime investigation. The court found that the Secret Service's conduct "resulted in the seizure of property, products, business records, business documents, and electronic communications equipment of a corporation and four individuals that the statutes were intended to protect."⁵ The court, clearly concerned about the government's conduct, recommended "better education, investigation, and strict compliance with the statutes as written."

Clearly, the decisions made by the Sentencing Commission regarding those factors that may increase or decrease a criminal sentence will have an important impact on how computer crime is understood and how the government conducts investigations. We therefore appreciate the opportunity to express our views on the proposed changes to the guidelines for 18 U.S.C. 1030.

For the reasons stated below, it our belief that the proposed guidelines regarding the Computer Fraud and Abuse Act now under consideration by the Sentencing Commission place emphasis upon the wrong factors, and may discourage the use of computer technology for such purposes as publication, communication, and access to government information. For these reasons, CPSR hopes that the current proposal will not be adopted.

³ S. Rep. 544, 101st Cong., 2d Sess. 4 (1990).

⁴ No. A-91-CA-346-SS (W.D. Tex. Mar. 12 1993).

⁵ Id. at 26-27.

The Proposed Guidelines Will have a Chilling Effect on Constitutionally Protected Activities

The proposed amendment would treat as an aggravating factor the alteration, obtaining, or disclosure of "Protected information." This term is defined in the proposed guidelines as "private information, non-public government information, or proprietary commercial information." The term is nowhere mentioned in the statute passed Congress.

We oppose this addition. It has been the experience of the computer profession that efforts to create new categories of information restriction invariably have a chilling impact on the open exchange of computerized data. For example, National Security Decision Directive 145, which gave the government authority to peruse computer databases for so-called "sensitive but unclassified information," was widely opposed by the computing community, as well as many organizations including the Information Industry Association and the American Library Association. The reason was that the new designation allowed the government to extend classification authority and to restrict the free flow of information and ideas.⁶

Clearly, this proposal to increase the sentence for a violation of a particular federal statute is not as sweeping as a Presidential order. Nonetheless, we believe that the problems posed by efforts to create new categories of computer-based information for the purpose of criminal sentencing will raise similar concerns as did NSDD-145. It is not in the interest of those who rely on information systems for the purpose of public dissemination to encourage the development of such classifications.

The proposed guidelines would also treat as an aggravating factor the alteration of public record information. This proposal may go directly against efforts to promote public access to electronic information and to encourage the use of computer networks for the conduct of government activities. For example, computer bulletin boards have been established by agencies, such as the Department of Commerce and Environmental Protection Agency, precisely for the purpose of encouraging public use of on-line services and to facilitate the administration of agency business.

⁶ See Military and Civilian Control of Computer Security, Hearing before the Legislation and National Security Subcomm. of the Comm. on Government Operations, House of Rep., 101st Cong., 1st Sess. (1989).

Much of the problem may well be with the use of the term "alter" without any further discussion of the nature of the alteration. Computer systems are by nature interactive. Any user of a computer system "alters" the data on the system. System operators may control the status of a particular file by designating it as a "read only" file or a "read-write" file. When a file is "read only," a user may access the file but is technically unable to alter the files contents. However a file that is "read-write" may allow users to both review files and to alter them.

Certainly, there are many other factors that relate to computer system security, but this particular example demonstrates that in many instances altering a public file may in fact be the intended outcome of a system operator. Failing to distinguish between permissible and impermissible alterations of a computer file in the sentencing guidelines misses entirely the operation of many computer systems.

The proposed amendment would also discourage the publication of information in electronic environments. The amendment recommends that the sentence be increased by 4 levels where "the defendant disclosed protected information to any person" and by six levels where "the defendant disclosed protected information to the public by means of a general distribution system."

Both of these proposals would punish the act of publication where there is no economic advantage to the defendant nor any specific harm indicated. Such provisions could be used to discourage whistle-blowing in the first instance, and subsequent dissemination of computer messages by system operators in the second.⁷

For this reason, we strongly oppose the inclusion of comment 10 which states that a "general distribution system" includes electronic bulletin boards and voice mail systems. This particular comment could clearly have a chilling effect on operators of electronic bulletin boards who may become reluctant to disseminate information where such dissemination could be considered an aggravating factor for the purpose of the federal computer crime law.

Current guidelines

It is our view that the current guidelines are a reasonably fair articulation of the specific harms that might warrant additional stringency, at least in the area of computer crime. We believe that it is appropriate to impose additional sanction where there is "more than minimal

⁷ See Steve Jackson v. Secret Service, supra.

planning" or "scheme to defraud more than one victim," as currently stated in the Guidelines. One of our concerns with the application of 18 U.S.C. 1030 after the decision in U.S. v. Morris, 928 F.2d 504 (2d Cir. 1991) is that the provision does not adequately distinguish between those acts where harm is intended and those where it is not. For this reason, provisions in the sentencing guidelines which help to identify specific harms, and not simply the disclosure of computerized information, may indeed be helpful to prosecutors who are pursuing computer fraud cases and to operators of electronic distribution systems.

For similar reasons, we support the current §2F1.1(4) which allows an upward departure where the offense involves the "conscious or reckless risk of serious bodily injury." Again, it is appropriate to impose a greater penalty where there is risk of physical harm.

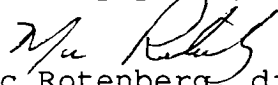
The Commission may wish to consider at some future date a provision which would allow an upward departure for the disclosure of personally identifiable data that is otherwise protected by federal or state statute. We believe that privacy violations remain an important non-economic harm that the Commission could address. For instance, the disclosure of credit reports, medical records, and criminal history records, by means of an unauthorized computer use (or where use exceeds authorization) may be an appropriate basis for the imposition of additional sanctions.

We suggest that the Commission also consider whether a downward departure may be appropriate for those defendants who provide technical information about computer security that may diminish the risk of subsequent violations of the computer fraud statute. Such a provision may lead to improvements in computer security and the reduced likelihood of computer-related crime.

We recognize that the Commission is currently considering factors that should be considered in the imposition of federal sentencing, and that this process should not be equated with the creation of new criminal acts. Nonetheless, the decisions of the Commission in this area may well influence subsequent legislation, and the ability of computer users to make use of information systems, to access government information, and to disseminate electronic records and files. It is for these reasons that we hope the Sentencing Commission will give careful consideration as to potential impact on the user community of these proposed changes to the federal sentencing guidelines.

We appreciate the opportunity to provide these comments to the Commission and would be pleased to answer any questions you might have. Please contact me directly at 202/544-9240.

Sincerely yours,

A handwritten signature in dark ink, appearing to read 'Mr. Rotenberg', written over the printed name.

Marc Rotenberg, director
CPSR Washington office

Enclosure

S. HRG. 101-1276
**THE COMPUTER ABUSE AMENDMENTS ACT OF
1990**

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED FIRST CONGRESS

SECOND SESSION

ON

S. 2476

A BILL TO AMEND TITLE 18 OF THE UNITED STATES CODE TO CLARIFY
AND EXPAND LEGAL PROHIBITIONS AGAINST COMPUTER ABUSE

JULY 31, 1990

Serial No. J-101-91

Printed for the use of the Committee on the Judiciary



CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	Page 1, 2
Humphrey, Hon. Gordon J., a U.S. Senator from the State of New Hampshire	41

PROPOSED LEGISLATION

S. 2476, a bill to amend title 18 of the United States Code to clarify and expand legal prohibitions against computer abuse	4
---	---

CHRONOLOGICAL LIST OF WITNESSES

Mark Richard, Deputy Assistant Attorney General, Criminal Division, Department of Justice, accompanied by William Esposito, section chief, White Collar Crimes Unit, FBI	10
John Pickitt, president, Computer and Business Manufacturers Association, Washington, DC	45
Douglas C. Jerger, director, Software Industry Division, ADAPSO, Arlington, VA	54
Marc Rotenberg, Computing and Civil Liberties Project, Computer Professionals for Social Responsibility, Washington, DC	62
David Johnson, law firm of Wilmer, Cutler & Pickering, Washington, DC	88

ALPHABETICAL LIST AND MATERIAL SUBMITTED

Jerger, Douglas C.: Testimony	54
Prepared statement	56
Johnson, David: Testimony	88
Prepared statement	90
Pickitt, John: Testimony	45
Prepared statement	46
Richard, Mark: Testimony	10
Prepared statement	12
Rotenberg, Marc: Testimony	62
Prepared statement	64, 74

APPENDIX

Letter to the Subcommittee on Technology and the Law, Committee on the Judiciary, from Robert H. Courtney, Jr., president, RCI, Port Ewen, NY 12466, November 5, 1990	109
---	-----

(III)

COMMITTEE ON THE JUDICIARY

JOSEPH R. BIDEN, Jr., Delaware, <i>Chairman</i>
EDWARD M. KENNEDY, Massachusetts
HOWARD M. METZENBAUM, Ohio
DENNIS DECONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois
HERBERT KOHL, Wisconsin
RONALD A. KLAIN, <i>Chief Counsel</i>
DIANA HUFFMAN, <i>Staff Director</i>
JEFFREY J. PECK, <i>General Counsel</i>
TERRY L. WOOTEN, <i>Minority Chief Counsel and Staff Director</i>

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

PATRICK J. LEAHY, Vermont, <i>Chairman</i>
GORDON J. HUMPHREY, New Hampshire
ANN M. HARKINS, <i>Chief Counsel</i>
GEORGE C. SMITH, <i>Minority Chief Counsel and Staff Director</i>

(II)

Senator LEAHY. Thank you, Mr. Jerger.
Go ahead, Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, COMPUTING AND CIVIL LIBERTIES PROJECT, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY, WASHINGTON, DC

Mr. ROTENBERG. Mr. Chairman, Senator Humphrey, thank you for the opportunity to testify today.

My name is Marc Rotenberg. I am director of the Washington office of Computer Professionals for Social Responsibility. I will speak briefly on three issues regarding S. 2476.

The first point I would like to make is that CPSR supports the proposed adoption of the recklessness provision in the computer crime law. We believe that this is a sensible way to send a message to the computing community that those acts which even though may not be malicious, which nonetheless result in harm because of someone's disregard for the needs of other users should be punished. For this reason, we would support the recklessness provision and the expansion of the scope of the computer crime law to cover those types—

Senator LEAHY. Expansion of—

Mr. ROTENBERG. Expand the scope of the law to cover those acts that involve clear recklessness.

Having said that, I should point out that while this provision is based in part on the experience with the *Morris* case, it is worth noting that the current law did cover the *Morris* case quite well. Robert Morris was convicted of a felony act, and under the Federal sentencing guidelines would have received a sentence of almost 2 years. So at least to those who say that the law is not adequate for the *Morris* situation, I think the facts suggest otherwise.

My second point is regarding the civil liberties implications of computer crime investigations. And, as you indicated earlier, Senator, the recent experience with Steve Jackson Games in Texas and with the Craig Neidorf prosecution in Chicago, suggests that at least in some instances Federal prosecutors have reached too far in the conduct of computer crime investigations. And I believe part of the reason for this may be a matter of terminology. We have become so accustomed to the thought that computer hacking is necessarily malicious or necessarily criminal that when the word "hacking" comes up, prosecutors appear to leap and look for an opportunity to conduct an investigation.

The point I would like to make is that there is nothing in title 18 that criminalizes computer hacking. Title 18 criminalizes unauthorized access to computer systems, and that is an important distinction that must be made so that prosecutors stay focused on the target and that people who have not committed an unlawful activity do not get swept up within the investigative net.

And my final point is simply this: There is clearly a problem of computer crime in this country. Estimates losses run between \$3 billion and \$5 billion a year, but losses of those amounts are tied to acts of individuals who for malicious purposes or purposes of self-gain take from others what is not rightfully theirs. Those are the acts that Federal prosecutors should be focusing on. Those are the

acts which cause the greatest harm to our economy. And we hope that in the ongoing work of the law enforcement agencies they will make sure that their priorities are in accord with that need.
Thank you, Mr. Chairman.

[The prepared statements of Mr. Rotenberg follow:]

Prepared Testimony
and
Statement for the Record

of

Marc Rotenberg
Director, Washington Office

Computer Professionals for
Social Responsibility (CPSR)

on

S. 2476

The Computer Abuse
Amendments Act of 1990

before

The Subcommittee on Technology and Law,
Committee on the Judiciary,
United States Senate

July 31, 1990

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today on the Computer Abuse Amendment Acts of 1990. My name is Marc Rotenberg and I am the director of the Washington Office of Computer Professionals for Social Responsibility.

CPSR is a national organization of computer scientists and other specialists that seek to inform the public about the social impact of computer systems. Our membership includes a Nobel Laureate and four winners of the Turing Award, the highest honor in computer science.

I also want to thank you, Senator Leahy and the other members of the Committee, for taking the lead on the computer virus issue. Your hearing last March with Cliff Stoll and FBI Director William Sessions has helped the public understand the complex issues of computer crime and has laid the foundation for appropriate Congressional action.

I have a lengthy statement that I ask be entered into the hearing record. This afternoon I would like to focus on three points regarding the proposed legislation and computer crime.

First, CPSR supports the proposed addition of a recklessness provision in the criminal code. This change should help deter those computer acts, which though not malicious, are outside the bounds of responsible computing and place other computer users at risk. CPSR believes that this provision will heighten the sense of ethical accountability within the computer user community. At the same time, we have some questions about other provisions in the bill that would expand the scope of law enforcement authority, define the term "access," and create an action for civil damages.

Second, the conduct of computer crime investigations will necessarily raise civil liberties concerns. There is already evidence that the Secret Service conducted a poorly conceived search of a small business in Austin, Texas. And there are unanswered questions about the impact of the recent Secret Services raids on the operation of computer bulletin boards and freedom of speech. We need to be sure

CPSR Testimony

1

S. 2476

that there are adequate procedural safeguards to ensure that important civil liberties interests - freedom of speech, privacy of communication, and due process protections - are not diminished in the efforts to respond to computer crime.

Third, even as the public continues to worry about highly publicized incidents of computer "hacking," it is important to restate that the majority of computer crime is committed by authorized users who embezzle company funds, steal proprietary information, and destroy corporate records. These crimes, though they rarely receive the attention of the national papers, should remain the primary concern of the law enforcement agencies.

PROPOSED CHANGES TO SECTION 1030

Creation of Recklessness Provision

CPSR supports the creation of the recklessness misdemeanor provision contained in S. 2476. We believe that such a provision is necessary to discourage acts with computer systems which, though not intended to cause harm, demonstrate such an extraordinary disregard for the sensible use of a computer system and that such harm in fact results.

Computer users today are increasingly operating in an interconnected world. Individual terminals are linked together through local networks and national networks. These networks facilitate the exchange of information and increase the utility of computer systems for all users. Most systems are designed to encourage open access and to promote the rapid exchange of data. The potential risk with this arrangement is that it leaves users vulnerable to viruses, worms, and similar programs that could cause harm to individual user's systems.

The Cornell Worm demonstrated the risk of a rogue program on a computer network. Individual users were required to disconnect from the network. During the period of time that the network was down, users could not exchange electronic mail, could not transfer files, and could not access information in other systems that might be necessary for their work.

CPSR Testimony

2

S. 2476

The law should make clear to computer users that potentially dangerous experiments cannot be conducted in an environment that places other users at risk. The computing community is based on trust. When a user acts with disregard for the needs of others, he or she has destroyed that trust. For this reason, we will support legislation that expands the scope of computer crime law to cover acts of clear recklessness.

Let me note, however, that while this provision is clearly based on the Cornell Worm incident, it is intended to provide prosecutors with an alternative method of prosecuting cases; it is not intended to "fill a gap" in the law. In the Cornell case, Mr. Robert Morris, Jr. was convicted of a felony act, and, under the federal sentencing guidelines, would have received a sentence of about two years. Current law covered the Morris case. The reason for the recklessness provision is to make clear to computer users that they should not engage in experiments that place other users at risk.

Change in Scope of Computer Crime Law

CPSR would oppose the extension of computer crime law to computers "used in interstate commerce or communication." We believe that the scope of the current law which is based on a "federal interest computer system" is adequate and that the Justice Department has failed to show that it is necessary at this time to expand the scope of computer crime law.

Very few cases have been brought under the section of the criminal code that would be amended by the Act now under consideration by this Committee. In fact, the Morris case was the first jury trial for a section 1030 indictment. Before expanding the scope of this provision, it is critical to show that the current law is not adequate and that reasonable law enforcement goals cannot be addressed adequately in the current framework.

It is also clear, as the indictments following the Secret Service raid demonstrated, that there are a variety of ways to prosecute computer crime. Section 1030 is simply one tool available to law enforcement officials. We need more case law to determine whether the many prosecutorial theories outlined in the Justice

CPSR Testimony

3

S. 2476

Department manual on computer crime are adequate before expanding the scope of section 1030.

There is a further problem with the proposed change and that is that computers are so ubiquitous that criminalizing unauthorized access to computer systems could apply to virtually any act in today's world. This provision would go much further than the federal wiretap law. Without clear contours and bright lines, such a law may fail to serve any useful purpose.

We would say that unless the Justice Department can demonstrate the need for this change, based on a clear and compelling need, the Congress should await the development of further case law under the current statute. But if the Department of Justice is granted additional authority then we would strongly urge the Committee to consider the creation of additional procedural safeguards to ensure that civil liberties and due process interests are not undermined in the course of the investigation of computer-related crime.

Creation of Access Definition

We support the effort to define the term "access" in section 1030. At the same time, we must caution against vague and ambiguous phrases that provide little guidance to computers users or system operators. Under the proposed definition, a user who simply glances at a computer screen has effectively gained access to that system, yet may have no ability to alter the contents of the system or to otherwise affect its operation. Such a definition is clearly too broad for any reasonable purpose.

One of the points that should be stressed here is that the definition of access will vary widely depending on the environment in which the system exists. Access restrictions for system maintained by an intelligence agency will be far more extensive than for a university which is still more restricted than a computer in one's home. The law needs to take account of these varying standards to ensure that the expectations for the system user and the system operator in a particular environment correspond with the legal requirements. There must almost be clear notice of access restrictions for computer users so that anyone who might be charged under this provision understands the law and is able to comply with it.

CPSR Testimony

4

S. 2476

We would be happy to work with the Committee to see if it might be possible to draft a definition that is clearer in its purpose and more limited in its scope.

Creation of Civil Liability Provision

CPSR takes no position on the proposed creation of a civil action for acts under section 1030. If this change will encourage institutions to improve security practices, then it is worthwhile and should be adopted. At the same time, we do not want the fear of civil liability to curtail the use of computers and the exchange of information.

We do need to find incentives to improve computer security and user accountability. Criminal sanctions alone are probably too harsh a penalty and unlikely to lead to the institutional changes that are necessary if computer security is to be improved. For this reason, civil liability may be a reasonable alternative.

CIVIL LIBERTIES CONCERNS RAISED BY COMPUTER CRIME INVESTIGATIONS

Operation Sun Devil

Mr. Chairman, I would like to turn the recent series of searches conducted by the Secret Service. Although it has been just a few months since this raid was undertaken -- and much of the relevant information has not yet been disclosed -- it raises a number of significant civil liberties questions we hope the Committee will bear in mind as it considers whether to expand the scope of the Computer Fraud and Abuse Act.

During the last two years, the Secret Service undertook an extensive investigation of computer "hackers," culminating in a nationwide raid on May 7 that involved 150 Secret Service agents in 24 cities. So far, these searches have led to only six arrests. In Atlanta, three men pled guilty last month to gaining illegal entry to BellSouth Computers. But at least two cases have raised troubling questions about the scope and conduct of Operation Sun Devil.

In March of this year, the Secret Service raided the offices of Steve Jackson, a small businessman in Austin, Texas, who produces fantasy role-playing games,

CPSR Testimony

5

S. 2476

similar to Dungeons and Dragons. The Secret Service seized three of Mr. Jackson's computers as well as the materials for his new game, GURPS CYBERPUNK. As a result of the raid, Mr. Jackson, was forced to lay-off half of his staff and to incur substantial business losses.

In a second case, in Chicago, Illinois, Craig Neidorf, a twenty-year-old college student and the publisher of an electronic newsletter was charged by the government with distributing an administrative document obtained from BellSouth. Although the federal government initially alleged an extraordinary conspiracy involving unauthorized computer access and the national phone network, last Friday federal prosecutors in Chicago decided to drop the case against Mr. Neidorf.

Both the Jackson and Neidorf cases raised significant civil liberties and First Amendment issues. For if the First Amendment extends to electronic speech, then it would be impermissible for the government to attempt a prior restraint on publication. We know from the Pentagon Papers case that the government could not reach into the printing room of the newspaper and attempt to turn off the presses. Yet, in these more recent cases involving computer-based publishing, the government actually confiscated the "presses" in an effort to suppress dissemination of information that would be widely available, if printed in paper form.

Mitchell Kapor, one of the pioneers of the personal computer industry, and John Perry Barlow established an organization, the Electronic Frontier Foundation, Inc., in part to examine some of the civil liberties issues that might be raised by Operation Sun Devil and related investigations. The Jackson and Neidorf cases demonstrate the importance of this effort and the need for adequate Congressional oversight to ensure that overly zealous law enforcement officials do not take advantage of the current climate of public concern to undertake investigations that are unsound or misguided.

Although we will have a great many more cases before the application of the First Amendment to digital media is determined, this recent introduction suggests the importance of watching these developments closely.

Implications of Computer Crime Investigations for Privacy

CPSR Testimony

6

S. 2476

A related problem is to ensure that there are adequate safeguards in place so that computer crime investigations are properly tailored to a specific, well-defined purpose. On the one hand, evidence of computer crime may be more easily concealed than other types of crime. Data is easily encrypted. Files can be readily copied and just as easily destroyed. There are various techniques to remove data from disks before a new user is able to gain access. For these reasons, law enforcement officials argue that changes in the law may be necessary to conduct investigations of computer crime.

At the same time, searches of computer systems are almost necessarily broader than searches of physical spaces. Much of the information that can be easily obtained is unrelated to the investigation. Where the computer operates as a bulletin board or messaging gateway, electronic mail of hundreds or thousands of users could be accessible. Also, the ease of copying data may encourage law enforcement agents to make a copy of all the electronic media taken in a search to see if there is evidence of other types of crime, unrelated to the initial investigation for which a warrant was obtained.

Most significant is that computer communications are particularly vulnerable to surveillance and monitoring. Computer mail unrelated to a particular investigation could be swept up in the government's investigation if the law is not carefully tailored. Back-up tapes may contain copies of thousands of electronic messages and files.

This is not a matter of speculation. Based on a letter from the Secret Service to Members of the House Judiciary Committee, we know that the Secret Service has developed a Computer Diagnostics Center to scan the contents of electronic media seized in computer crime investigations. We would like to know if there are any restrictions on the use of the CDC, and whether, for example, the CDC is used to scan the contents of public bulletin boards in those cases where no warrant has been obtained.

Congress recognized the potential problem of searches of electronic media when it first considered the proper scope of electronic surveillance. That is the reason for the extensive system of procedural safeguards and the fundamental goal

CPSR Testimony

7

S. 2476

of minimizing the scope of searches that is mandated by section 2518 of the criminal code. These principles were carried forward and updated in the revisions that you, Mr. Chairman, helped enact with the Electronic Communication Privacy Act. ECPA drew a reasonable balance between the needs of law enforcement investigators and the rights of all computer users.

We would oppose any efforts at this time to modify the restrictions in ECPA, absent a showing that the law enforcement needs cannot be accommodated in some other fashion that does not undermine the privacy and security of computer systems.

We hope, at some point, that the Committee will conduct an oversight hearing on the ECPA and determine whether law enforcement officials are following the standards established in the 1986 law.

COMPUTER CRIME PROBLEM IS WIDELY MISUNDERSTOOD

My last point, Mr. Chairman, is to urge the Committee and the law enforcement community to direct its energies to those forms of computer-related crime that cause the greatest harm and that are based on malicious intent. These are the crimes of fraud, embezzlement, and theft that make up an estimated loss of \$3 to \$5 billion annually in this country.

It is a popular misconception that computer crime is caused primarily by young kids, technically skilled. One state assistant attorney general has actually stated that there is little difference between a teenager with a computer modem and a criminal with a handgun. And the FBI is now encouraging parents to help identify the early warning signs of "computer hacking."

The Secret Service has painted its case in broad strokes. "Computer hacking" is not a crime. Gaining unauthorized access to a federal interest computer system under section 1030 is. It is critical that this distinction not be lost. Once we lose our focus on prosecutable crime, the image blurs, and anyone may become the target of a law enforcement investigation.

CPSR Testimony

8

S. 2476

Those people who have violated the law should be held accountable. But so too should law enforcement officials who are bound by oath of office. It is a core principle of our constitutional form of government that the investigation of unlawful activity must be conducted by lawful means.

Thank you, Mr. Chairman, for the opportunity to testify today. I would be pleased to answer your questions.

CPSR Testimony

9

S. 2476

Prepared Testimony and Statement for the Record on Computer Virus Legislation*

Marc Rotenberg
Director, Washington Office
Computer Professionals for Social Responsibility (CPSR)
1025 Connecticut Avenue, NW
Suite 1015
Washington, DC 20036

Mr. Chairman, members of the Committee, thank you for the opportunity to testify on legislation regarding computer viruses. My name is Marc Rotenberg and I am the director of the Washington Office of Computer Professionals for Social Responsibility (CPSR).

CPSR is a national membership organization of computer scientists and other specialists that seek to inform the public about the social impact of computer systems. Our membership includes a Nobel Laureate and five Turing Award winners, the highest honor in computer science. CPSR members have examined several national computing issues and prepared reports on funding priorities in computer science, the Strategic Defense Initiative, computer risk and reliability, and the proposed expansion of the FBI's records system.¹

You have asked me to examine legislation that has been introduced in the House of Representatives.

* Before the Subcommittee on Criminal Justice, Committee on the Judiciary, US House of Representatives.

tives related to computer viruses. I appreciate this opportunity and am glad that you have taken an interest in this subject.

It was just a year ago last week that the Cornell "virus" swept through the Internet.² For many people in this country it was the first that they had heard of computer viruses and similar programs that could bring a nation-wide computer system to a halt. Even as system managers were clearing the code out of their computers, discussions about the vulnerabilities of computer systems and the rights and responsibilities of computer users were taking place all across the country.

CPSR Members Address the Computer Virus

In Palo Alto, California CPSR members met shortly after the Internet virus to discuss the significance of the event. Over the course of several days our members discussed the wide-ranging issues raised by the incident.³ The discussion revealed many concerns about network security, ethical accountability, and com-

puter reliability. It also revealed a division within our organization about the moral responsibility of the virus author. Some of our members believed that the person responsible for the virus had performed a great service for the computer community by drawing attention to the security flaws in the Internet, particularly the UNIX operating system. Others felt strongly that this person had violated a fundamental understanding within the computer community not to exploit known security flaws and had caused great damage to users of the Internet. The division within our organization reflected a division within the computer science community.⁴

In the end we issued a statement on the computer virus that has been widely circulated in the computer community and republished in computer journals.⁵ I have attached the CPSR statement to my testimony and ask that it be entered into the hearing record.

On the issue of the culpability of the person responsible for the virus we said clearly that the act was irresponsible and should not be condoned. The author of the virus had treated the Internet as a laboratory for an untested experiment in computer security. We felt this was very risky, regardless of whether data was altered or destroyed.

But we did not view our task primarily as sitting in judgement over the author of the Internet virus. There had been other viruses in the past, and there would be more in the future. More important, we believed, was to set out the various concerns of our organization for the public, policy makers, and others within the profession who were examining the significance of the computer virus and considering various responses. We reached the following conclusions:

First, we emphasized individual accountability as the cornerstone of computer ethics. We said that the openness of computer networks depends on the good will and good sense of computer users. Criminal penalties may be appropriate for the most pernicious acts of computer users. But for the vast majority of cases, far more would be accomplished by encouraging appropriate ethical guidelines.

Second, we said that the incident underscored our society's growing dependence on complex computer networks. Although the press and the public tended to focus on the moral culpability of the virus writer, we believed that the incident also raised significant policy questions about our reliance on computer systems. Since its inception, CPSR has been particularly concerned about the development of complex computer systems, especially in the military, that are difficult to test and may produce misplaced trust. There is little that tougher criminal penalties can do to correct the problems of computer risk and reliability.

Third, we opposed efforts to restrict the exchange of information about the computer virus. Shortly after the virus incident, officials at the National Security Agency (NSA) attempted to limit the spread of information about the computer virus and urged Purdue University to destroy copies of the virus code.⁶ We thought this was short-sighted. Since that time, several technical reports and the widespread exchange of information through the Internet have helped users in the computer community more fully understand how the virus operated and provided the necessary data to correct security flaws.⁷ We continue to believe that the needs of network users will be better served through the open and unrestricted exchange of technical information.

The importance of open computer networks was also demonstrated recently during the earthquake in the San Francisco Bay area. Before the national networks were able to report on the unfolding events, computer users were dialing up networks to search for friends and to reassure relatives. According to one account, a user of the Prodigy service in the Bay Area sent a message out through the network to subscribers in central Kansas, asking that someone pass the word on to his son, a soldier based at Fort Riley, that everybody back home was ok. The soldier, who had been unable to reach home, received the message from a complete stranger.⁸

Fourth, we encouraged a public discussion about the vulnerabilities of computer networks and the various technical, ethical, and legal questions raised by the incident. Since the meeting, CPSR members, along with others in the computer community, have been involved in a variety of activities, hosting panel discussions on the virus incident, drafting papers, and encouraging an examination of ethical standards. We believe that these efforts will help develop a broader understanding of the rights and responsibilities of network users.

Complexity of the Virus Problem

I will this morning describe some of the concerns of the computer community and make several recommendations about what Congress might do to respond to the problem of computer viruses. I will also address some of the potential problems posed by proposed federal legislation. At the outset, I should make one fundamental point: The problems raised by computer viruses are far-reaching and complex. There is no simple technical or legal solution. In many ways, we are confronting a whole new series of policy questions that raise fundamental issues

about privacy and access, communications and accountability. Public policy must be brought up to date with new technologies, but in the effort to ensure that our laws are adequate Congress should not reach too far or go off in directions that are mistaken or may ultimately undermine the interests we seek to protect.

There are several issues that should be considered in the efforts to develop appropriate legislation to respond to malicious code. First is the increased interdependence of computer systems. The technological developments that makes possible the spread of computer viruses also makes possible the transfer of vast amounts of computer information. Through computer networks, we are now able to send electronic mail, research findings, and tips on security fixes far more rapidly than ever before. Efforts to restrict the exchange of computer viruses run the risk of limiting the flow of this valuable information.

Throughout the computer community, there is a deep concern that solutions to computer security problems not destroy the trust between computer users. Ken King, the President of EDUCOM has warned against short-sighted solutions.⁹ Cliff Stoll, the Berkeley astronomer turned computer security expert, speaks of the need to preserve honesty and trust within the computer community and warned against measures that could restrict exchange of computer communications.¹⁰

As computer networks have developed, so has our concern about the reliability of computer systems. We must reexamine our growing dependence on complex computer networks, particularly in the military. Simply put there are too many computer systems in use today that are dangerously unstable.¹¹ A report produced recently by the staff of the Subcommittee on

Investigations and Oversight of the House Science Committee highlights the enormous risk of the current software development process.¹² We are automating too many complex problems with the expectation that computer systems can solve problems that we ourselves don't fully understand. In areas that involve life critical functions, the consequences of computer error could be great.¹³

I raise these issues because there is a need to be wary of quick legal or technical fixes that do little to address the underlying problems we must confront. There is a widely shared belief among computer security experts that there is no "silver bullet" that will solve the problem of computer viruses.¹⁴ Though there is much that can be done to improve computer security and operations, it should be understood that no system will ever be one hundred percent secure.

Need for Teaching Computer Ethics

A large part of the task that lies ahead is to develop a system of ethics that teaches computer users about the appropriate uses of computer systems. We need to discourage computer users from making use of shared resources in ways that make systems less useful to others. To suggest an approach to computer ethics that avoids some of the shortcomings of legislation based on rapidly changing technical terms or ambiguous legal phrases I would like to set out an elaborate analogy. The more I have tried to understand this issue, the more I have been struck by the similarity between our evolving computer networks and interconnected databases, and our public libraries.

A library provides a great wealth of information for its users, but not all information is equally accessible. In many libraries, I can freely roam

the stacks and pull out what I need. But other libraries might require that I put my request on paper before the materials are delivered. Certain materials at a reference desk are only accessible after I have spoken with the appropriate person and obtained permission.

A computer system operates in much the same way. On many systems, I am allowed to look through large reams of data without harm to anyone. But for certain information, I need permission. If I were to reach over the reference librarian's desk to take an article I wanted or to look at circulation records, I would be violating a library rule. So too, does the computer user violate a computer rule when he or she enters a system's operating system, knowing that only system managers and other privileged users are authorized. We need to remind system users about the difference between space that is public and that which is private.¹⁵

There are also other users in the library. In some libraries, users might be asked to leave books in study carrels so that others can find them. But my right to look at a book in another person's carrel would not extend to a right to go through the person's book bag. Similarly, it may be perfectly appropriate to look at another person's computer files if it is clear that they are publicly accessible, as long as I do not go through the person's private files.

A library also relies on the trust and good will of its users. A person who steals a book, or tears a page out of a magazine has not just caused harm to the library, but has deprived other users of the library or a valuable resource. Computer users, like users of a library, must increasingly understand the consequences of their actions in terms of the needs and activities of others.

Of course it is worth noting that there are laws against theft of library materials and destruction of library resources. But neither these laws nor the threat of prosecution have much effect on the habits of library users, since the likelihood of prosecution is so remote. When sanctions are imposed, it is by the library and not the federal government.

Partial Solutions

The complexity of the computer virus problem requires a multi-part approach. Computer users, system managers, vendors, professional organizations, educators, and the government all have a role to play.

In the federal government much is happening, though more could be done.¹⁶ The National Institute of Standards and Technology (NIST) recently prepared a special publication on computer viruses intended for managers of federal computer systems that is useful and easy to read.¹⁷ It should be made widely available for all of the federal agencies.

Another step that has been taken is the development of the Computer Emergency Response Team (CERT). The proposal was developed last December at a closed-door session with UNIX users and vendors at the National Computer Security Center.¹⁸ While it is good to see the cooperative undertaking between the federal government and the user community, it is not an ideal arrangement. CERT operates through the National Security Agency and the Department of Defense. Military control of computer security is precisely what Congress tried to avoid with the passage of the Computer Security Act.¹⁹ As CPSR has noted in the past, broad claims of national security should not provide carte blanche for the Department of Defense and

intelligence agencies to extend their authority over computer security.²⁰

Moreover, it is not even clear that CERT's advice is error-free. A recent posting to the "Risks" computer bulletin board on the Internet noted that CERT had mistakenly sent out an advisory to network users recommending the use of potentially infected system utilities to correct known security flaws. As one computer user noted, this was not good advice.²¹

The General Accounting Office (GAO) produced a useful overview of virus issues in a report released in June.²² The GAO recommended that the White House Science Adviser assume responsibility for improving computer security.

Although the GAO's concerns about lax security practices is well taken, I suspect that many users in the computer science community would object to centralizing authority for computer security for several reasons. Based on the experience with the Internet, it seems that the university and research community, Berkeley and MIT in particular, were more effective in responding to the virus than the federal agencies.²³

One of the lessons of the Internet virus is that responses should be developed at the host level and not the network level. As Jeff Schiller, the manager of the MIT Network and Project Athena Operations Manager, has said "anybody can drive up to your house and probably break into your home, but that does not mean we should close down the road or put armed guards on exit ramps."²⁴

The great value of the Internet for the user community is its decentralized structure. Like the phone network, it provides rapid access for users across the country. System security requirements will vary from site to site, depending

on whether the user is located at a university, in private industry, or a military agency. If the GAO recommendations are followed, it should only be to strengthen the flow of information about network security. Any steps to create a coercive authority in the White House for computer security on the Internet, such as the creation of a computer security czar, would be a serious mistake.

Universities and research institutions can also take steps to ensure that adequate policies are established to minimize the risk of computer viruses. Universities that fail to take reasonable steps to ensure that their systems are not used for the perpetration of a virus may find themselves civilly liable under tort law.²⁵ Many universities have already established policies that outline the responsibilities of users of computer facilities, which can serve as models for other schools.²⁶

Research in computer ethics will also help reduce the likelihood of computer misuse. The National Science Foundation is planning a major conference to bring together leaders in the computer science community and philosophers to discuss how more might be done to incorporate ethics into computer education. This is a sensible undertaking and should build upon the work that has already been done to improve computer ethics.²⁷ At the same time, it is important to note that much of the discussion about computers and ethics focuses on the responsibilities of individual users of computer systems and not on the large organizations or institutions that maintain and operate these systems. A coherent system of ethics that binds a community of users, like a system of democratic government, must be based on an implied contract between the individual and the institution. The individual will uphold his or her responsibility if the institution does as well. Concerns about privacy, security,

data quality and accountability should also be addressed as institutions move forward with their recommendation for computer ethics.

Review of Legislation

The last five years has been a period of rapid development in computer security legislation. Congress has three times passed laws designed to extend criminal statutes to computer technology.²⁸ Virtually all of the states have adopted new statutes, and many are looking at possible changes and additions.²⁹ There are available to prosecutors today a wide range of theories to base criminal charges for computer related crime.³⁰

Based on the views of CPSR members, the experience of the Internet virus, and our general concern about protecting open computer networks, I will describe the potential problems with the proposed federal legislation.

It is important to remember that a computer virus may also be a form of speech, as was the Aldus Peace Virus, and that to criminalize such activities may run afoul of First Amendment safeguards. Restrictions on speech should be carefully examined to ensure that free expression is not suppressed. Computer networks are giving rise to new forms of communication. The public debates in the town square of the eighteenth century are now occurring on the computer networks that will take us into the twenty-first century. These are fragile networks, and the customs and rules are still evolving. The heavy hand of the government could weaken the electronic democracy that is now emerging.³¹

Our legal system protects the fundamental right of free speech in a democratic society and gives special attention to laws that may unduly restrict

the exchange of information. It would be wrong to criminalize a computer communication if the communication caused no damage, even if the communication did not follow traditional pathways. It is often those individuals and organizations without great resources who turn to these alternative methods of communication to convey a message.

I wonder also if in casting such a broad net, these statutes might not meet constitutional challenge on overbreadth grounds.¹¹ A criminal law should clearly distinguish between prohibited and permissible conduct. If it fails to do this, it grants too much discretion to law enforcement officials to choose which cases to prosecute. Where speech is involved, such a law might unnecessary chill protected speech.

Some of the state statutes are poorly conceived. Those with the software trade association who have been pushing to extend the reach of computer security statutes might consider whether the products of their own members violate restrictions on "alteration of data" or "unauthorized use of resources."¹² To some extent, every computer program takes control of the user's systems. If the program acts as intended, then there are no problems. But if the program misfires, as it sometime does, software developers may be criminally liable.

A further problem lies in the attempt to define the criminal act in terms of a technical phrase such as a "virus." A virus is not necessarily malicious. Some viruses may only display a Christmas greeting and then disappear without a trace.¹³ Other viruses might alter or destroy data on a disk. To treat the two acts as similar because an identical technique is involved would be similar to punishing all users of cars because some cars might cause the death of a person. It

is the "state of mind" of the actor and the harm that results which should be the two guiding principles for establishing criminal culpability.¹⁴

More interesting from a technical viewpoint is that computer viruses may be used both to enhance computer security and to facilitate the exchange of computer information.¹⁵ Although computer security experts have said that such programs are potentially as dangerous as the disease they are designed to cure,¹⁶ it is not clear the disseminating a benign virus should necessarily be a criminal act. Hebrew University used a computer virus to identify and delete a malicious virus that would have destroyed data files across Israel if it had remained undetected.¹⁷

I would recommend that the Congress wait until there is more case law under the 1986 Act and until more of the state statutes have been tested, before enacting new computer security legislation. Congress should also obtain information from the Justice Department about the effectiveness of the current laws, and see whether state courts can develop common law analogies to prosecute the computer equivalents of trespassing, breaking and entering, and stealing.¹⁸ This is a process that happens gradually over time. The extension of common law crimes to their computer equivalents may provide a more durable and lasting structure than federal statutes that must be updated every couple of years.

Funding

It is difficult to talk about the role of Congress in improving computer security without noting the importance of funding to implement the Computer Security Act, the law passed by Congress designed to address the computer security needs of the federal agencies. I was very disturbed to learn two weeks ago that the conference commit-

tee cut the proposed appropriation for NIST from \$6 million to \$2.5 million, even after OMB had approved the funding for NIST and encouraged NIST's new role as the lead agency for civilian computer security.¹⁹ According to one news account, the cut came at the urging of a Member who had tried unsuccessfully to redirect part of NIST's 1989 appropriation to a special research testing facility in his home state. If this news account is accurate, then that Member's shortsighted and parochial concerns may cost the federal agencies dearly in needed assistance with computer security.

Conclusion

I believe that Peter Neumann, a computer security experience at SRI and a member of CPSR, described the problem best when he said:

Better laws that circumscribe malevolent hacking and that protect civil and constitutional rights would be of some help, but they cannot compensate for poor systems and poor management. Above all, we must have a computer-literate populace — better educated, better motivated and more socially conscious.²⁰

Tougher criminal penalties may help discourage malicious computer activities that threaten the security of computer networks, but they might also discourage creative computer use that our country needs for technological growth.²¹

Though we have a great deal of criminal law that could potentially apply to the acts of computer users, it is still very early in the evolution of computer networks. In the rush to criminalize the malicious acts of the few we may discourage the beneficial acts of the many and saddle the new technology with more restrictions than it can withstand.²²

Footnotes

¹ More information about CPSR is available from the CPSR National Office (P.O. Box 717, Palo Alto, CA 94302, (415) 322-3778) and the CPSR Washington Office (1025 Connecticut Ave., NW, Suite 1015, Washington, DC 20036, (202) 775-1588).

² It should be noted that there is a debate within the computer community about the correct term to apply to the program that travelled across the Internet. Purists, following the established taxonomy of computer security, prefer the term "worm" because the Internet program did not attach itself to another program, as viruses technically do, but rather was a free-standing program that infiltrated the network. However, the broad scope and rapid rate of the program's impact suggested to many that the term "virus" was more descriptive than "worm." The press and many within the computer community followed this usage.

³ John Schmerdewald, "The Virus Perpetrator: Criminal or Hero?" *The San Francisco Chronicle*, November 23, 1988, at C1.

⁴ Compare Aaron Haber, "Give No Quarter to Creator of Computer Virus," *PC Week*, December 5, 1988, editorial, "Faint Praise," *Computerworld*, November 14, 1988, at 24, Edwards A. Parrish, "Breaking Into Computers Is A Crime - Pure and Simple," *Los Angeles Times*, December 4, 1988 (Dr. Parrish is dean of the Vanderbilt University School of Engineering and President of the IEEE Computer Society), Jon A. Rochlis and Mark W. Eichin, "With Microscope and Tweezers: The Worm from MIT's Perspective," *32 Communications of the ACM* 689, 697 (June 1989).

⁵ "CPSR Statement on the Computer Virus," *The CPSR Newsletter* 2-3 (Winter 1989), reprinted in *32 Communications of the ACM* 699 (June 1989). The virus incident caused several other organizations to examine the need for ethical standards. See, e.g., "NSF Poses [sic] Code of Networking Ethics," *32 Communications of the ACM* 688 (June 1989) (National Science Foundation code), "Teaching Students About Responsible Use of Computers," *32 Communications of the ACM* 704 (June 1989) (describing the statement of ethics for MIT's Project Athena), "Ethics and the Internet," *32 Communications of the ACM* 710 (June 1989) (Internet Activities Board code).

Several national data processing, computer, and engineering organizations had well established codes prior to the virus incident. See "DPMA Code of Ethics, Standards of Conduct and Enforcement Procedures," (Data Processing Management Association), "ACM Code of Professional Conduct: Procedures for the Enforcement of the ACM Code of Professional Conduct," (Association for Computing Machinery), "IEEE Code of Ethics," (Institute of Electrical and Electronics Engineers), reprinted in *Proceedings of the 12th National Computer Security Conference* 547-52 (1989).

⁶ John Markoff, "U.S. Moving to Restrict Access to Facts About Computer Virus," *The New York Times*, November 11, 1988.

⁷ See, e.g., Jon A. Rochlis and Mark W. Eichin, "With Microscope and Tweezers: The Worm from MIT's Perspective," *32 Communications of the ACM* 689 (June 1989), Don Seeley, "A Tour of the Worm," (November 1988) (Department of Computer Science, University of Utah), Eugene H. Spafford, *The Internet Worm Program: An Analysis*, *Purdue Technical Report* CSD-TR-823

(Nov. 28, 1988), reprinted in *19 Computer Communications Review* 1 (January 1989). See also Spafford, "Crisis and Aftermath," *32 Communications of the ACM* 678 (June 1989). John Markoff, "The Computer Jam: How It Came About," *The New York Times*, November 9, 1988, at D10. See generally, *Proceedings: 1988 IEEE Symposium on Security and Privacy*, *Proceedings: 1989 IEEE Symposium on Security and Privacy*.

Two computer conferences on the Internet have been a valuable source of information about computer security. Conference subscribers send information to the conference moderator, who then compiles the messages and sends postings to all subscribers. The "Virus-L" conference, moderated by Ken van Wyk at Lehigh University, contains information about specific viruses. The internet address for the conference is VIRUS-L@IBM1.CC.LEHIGH.EDU and administrative questions should be sent to krw@SEI.CMU.EDU. The "Risks" conference ("Forum on Risks to Public in Computers and Related Systems") provides more general information about computer risk and reliability. The moderator is Peter Neumann at SRI. The internet address is RISKS@CSL.SRI.COM.

⁸ T.R. Reid, "Bulletin Board Systems: Gateway to Citizenship in the Network Nation," *The Washington Post*, November 6, 1989, at 27 (Washington Business section).

⁹ King, K.M. "Overreaction to External Attacks on Computer Systems could be More Harmful than the Viruses Themselves," *Chronicle of Higher Education*, November 23, 1988, at A36.

¹⁰ Cliff Stoll, *The Cuckoo's Egg* 302-03, 311 (1989). See also, Cliff Stoll, Testimony on Computer Viruses, The Subcommittee on Tech-

nology and the Law, Committee on the Judiciary, United States Senate, May 15, 1989.

¹¹ See, e.g., "Proposed NORAD Computer System Called Flawed," *The Washington Post*, December 16, 1988, at A22.

¹² "Bugs in the Program: Problems in Federal Government Computer Software Development and Regulation," Staff study by the Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives, August 3, 1989. See also Evelyn Richards, "Study: Software Bugs Costing U.S. Billions: Document is Critical of Government's Role," *The Washington Post*, October 17, 1989, at D1.

CPSR has been engaged in an ongoing review of the problems of computer risk and reliability, particularly in defense-related systems. See, e.g., *Computers in Battle: Will They Work?* (1987) (edited by Gary Chapman and David Bellin), *Risk and Reliability: Computers and Nuclear War* (1986) (videotape available from CPSR), and *Losing Control?* (1989) (videotape available for CPSR).

¹³ Peter G. Neumann, "A Glitch in Our Computer Thinking: We Create Powerful Systems With Pervasive Vulnerabilities," *The Los Angeles Times*, August 2, 1988, part II, at 7. See also Ken Thompson, "Reflections on Trusting Trust," *27 Communications of the ACM* 761 (August 1984) (1983 ACM Turing Award Lecture).

¹⁴ John Markoff, "Virus Outbreaks Thwart Computer Experts," *The New York Times*, May 30, 1989, at C1.

¹⁵ Computer security experts take a slightly different approach to this problem. They speak

of "least privilege" which means allowing users to have access to only those files of the system for which they are authorized. Following this approach, it is possible to develop elaborate security schemes, based on a hierarchy of privileges, that clearly describe the privileges of each user. This model is appropriate for many large systems, but may be too formal for other computer systems, such as community bulletin boards, where there is little difference in the status of various system users.

¹⁶ Even as new programs are being developed to respond to computer viruses, it is disappointing to see that some system managers have failed to correct known security flaws that were exposed by the Internet virus last year. A rogue program recently attacked the same security holes at NASA that had been exploited last fall. John Markoff, "Computer Network at NASA Attacked by Rogue Program," *The New York Times*, October 7, 1989.

¹⁷ John P. Wack and Lisa J. Carnahan, *Computer Viruses and Related Threats: A Management Guide* (August 1989) (NIST Special Publication 500-166). The report can be ordered from NIST at (202) 783-3228 or through the Superintendent of Documents, Washington, DC 20402-9325 (stock number 003-003-02935-6). See also Stanley A. Kurzban, "Viruses and Worms — What Can you Do?" *7 ACM SIG Security Audit and Control Review* 16 (Spring 1989). For more general information about computer security policy, see Charles K. Wilk, *Defending Secrets Sharing Data: New Locks and Keys for Electronic Information* (October 1987) (Office of Technology Assessment), Louise G. Becker, *Computer Security: An Overview of National Concerns* (February 1983) (Congressional Research Service).

¹⁸ Martin Marshall, "Virus Control Center

Proposed," *Infoworld*, December 12, 1989, at 8. See also General Accounting Office, *Computer Security: Virus Highlights Need for Improved Internet Management*. 24-25 (June 1989) (GAO/IMTEC-89-57).

¹⁹ See Computer Security Act of 1987: Hearings on H.R. 145 Before a Subcommittee of the Committee on Government Operations, House of Representatives, 100th Cong., 1st Sess. 525-26, 456, 23 (statements of Congressman Brooks, Congressman Glickman, and Congressman English).

Prior to passage of the Computer Security Act, President Reagan attempted to establish primary computer security authority at the National Security Agency and to expand government classification authority under NSDD-145. Agents visited private information vendors and public libraries, and the free flow of information diminished. See Bob Davis, "Federal Agencies Press Data-Base Firms to Curb Access to 'Sensitive' Information," *The Wall Street Journal*, January 28, 1987; Judith Axler Turner, "Pentagon Planning to Restrict Access to Public Data Bases," *The Chronicle of Higher Education*, January 21, 1987; Connie Oswald Stofko, "Inquiry by FBI Causes Libraries to Assess Records," *SUNY Reporter*, February 12, 1987; Jerry J. Berman, "National Security vs. Access to Computer Databases: A new Threat to Freedom of Information," *2 Software Law Journal* 1 (1987). The NSA also approached election officials and investigated computerized vote-counting software. Burnham, "US Examines if Computer Used in '84 Elections is Open to Fraud," *The New York Times*, September 24, 1985, at A17.

Library associations, public interest organizations, and experts on information policy de-

scribed the risks of reduced access to information under NSDD-145. See American Library Association, *Less Access to Less Information by and about the U.S. Government* (1988); Steven L. Katz, "National Security Controls, Information, and Communications in the United States," *4 Government Information Quarterly* 63 (1987); People for the American Way, *Government Secrecy: Decisions without Democracy* (1987); John Shattuck & Muriel Morisey Spence, *Government Information Controls: Implications for Scholarship, Science and Technology*, excerpted in "When Government Controls Information," *91 Technology Review* 62 (April 1988).

The Computer Security Act followed widespread public opposition to NSDD-145. See House Committee on Science, Space, and Technology, H.R. Rep. No. 153, pt. 1, 100th Cong., 1st Sess. 18, 19 (1987), reprinted in 1988, U.S. Code Congressional and Administrative News 3133, 3134, 3133 (Statement of Jack W. Simpson, President, Mead Data Central; statement of John M. Richardson, Chairman, Committee on Communications and Information Policy, Institute of Electrical and Electronic Engineering; statement of Cheryl W. Helsing, American Bankers Association). See generally Marc Rotenberg, Testimony on the Computer Security Act, Before the Subcommittee on Legislation and National Security, Committee on Government Operations, U.S. House of Representatives 2-5, May 4, 1989.

²⁰ See Mary Karen Dahl, "'Sensitive, Not 'Secret': A Case Study," *5 CPSSR Newsletter* 1 (Fall 1987); Marc Rotenberg, Testimony on the Computer Security Act, Before the Subcommittee on Legislation and National Security, Committee on Government Operations, U.S. House of Representatives, May 4, 1989; Letter to Representative Dan Glickman from Marc Roten-

berg regarding NSA efforts to suppress dissemination of encryption technology, August 18, 1989. See also "Computer Security Questioned," *The Baltimore Sun*, April 10, 1989, at A7.

²¹ Anonymous, "Warning About CERT Warnings," *9 Forum on Risks to the Public in Computers and Related Systems* 36 (October 27, 1989) (Internet computer conference) (moderated by Peter Neumann).

²² General Accounting Office, *Computer Security: Virus Highlights Need for Improved Internet Management* (June 1989) (GAO/IMTEC-89-57). See also statement of Jack L. Brooks, Director, Government Information and Fiscal Management Issues, Information Management and Technology Division, Hearing Before the Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives, July 20, 1989.

²³ Jon A. Rochlis and Mark W. Eichin, "With Microscope and Tweezers: The Worm from MIT's Perspective," *32 Communications of the ACM* 687, 697 (June 1989).

²⁴ *Ibid.*

²⁵ See American Council on Education and United Educators Insurance, *A White Paper on Computer Viruses* (May 1989) (prepared by David R. Johnson, Thomas P. Olson, and David G. Post). See also "The Computer Worm: A Report to the Provost of Cornell University on an Investigation Conducted by the Commission of Preliminary Enquiry" (February 1989) (Cornell University).

²⁶ See, e.g., *Handbook for Students, Harvard College 1987-1988* 85 ("Misuse of Computer Systems").

²⁷ See, e.g., Donn B. Parker and Bruce N. Baker, "Ethical Conflicts in Information and Computer Science, Technology and Business" (August 1988), Deborah Johnson and John W. Snapper, *Ethical Issues in the Use of Computers* (1985), Glenda Eoyang, "Acquisition and Maintenance of Ethical Codes," and John Ladd, "Ethics and the Computer Revolution," *DIAC-88: Directions and Implications of Advanced Computing 102, 108* (Computer Professionals for Social Responsibility 1988) (edited by Nancy Leveson and Douglas Schuler).

²⁸ In October 1984, the Computer Fraud and Abuse Act was signed into law. P.L. 99-473 and 99-474 codified at 18 U.S.C. 1030. In 1986 the law was amended and expanded to include "federal interest computers." A companion statute addresses fraud and related activity in connection with an access device. 18 U.S.C. 1029. See also Electronic Communications Privacy Act of 1986, particularly 18 U.S.C. 2510 ("Wire and electronic communications and interception oral communications") and 18 U.S.C. 2701 ("Unlawful access to stored communication").

²⁹ See Anne W. Branscomb, *Rogue Computer Programs - Viruses, Worms, Trojan Horses, and Time Bombs: Pranks, Prowess, Protection or Prosecution?* 20-28, 33-42 (September 1989) (Program on Information Resources Policy, Harvard Center for Information Policy Research). Another useful source is the Congressional Research Service report by Robert Helfant and Glenn I. McLoughlin, "Computer Viruses: Technical Overview and Policy Considerations" (August 15, 1988) (88-556 SPR).

³⁰ See Branscomb at 28-31. See also Department of Justice, *Computer Crime: Legislative Resource Manual* (Bureau of Justice Statistics).

³⁸ A compelling argument for the need to avoid restrictions on electronic communication can be found in Itzhak de Solà Pool, *Technologies of Freedom* (1983).

³⁹ See Lawrence Tribe, *American Constitutional Law* 1022-39 (2nd ed. 1988).

⁴⁰ The president of an organization of programmers called the Software Development Council has stated, "release a virus, go to jail." "Invasion of the Data Snatchers!" *Time*, September 26, 1989, at 67.

⁴¹ The so-called Aldus Peace Virus is an example of a benign virus. See Anne W. Branscomb, *Rogue Computer Programs - Viruses, Worms, Trojan Horses, and Time Bombs: Pranks, Prowess, Protection of Prosecution?* 5-6 (September 1989) (Program on Information Resources Policy, Harvard Center for Information Policy Research).

⁴² See Wayne R. LaFare and Austin W. Scott, Jr., *Criminal Law* 5-6 (1972).

⁴³ Indeed, someday a computer virus might be needed to free society from tyrannical rule. John Brunner, *The Shockwave Rider* (1975).

⁴⁴ John Markoff, "Computer Virus Cure May Be Worse Than Disease," *The New York Times*, October 7, 1989, at A1.

⁴⁵ Anne W. Branscomb, *Rogue Computer Programs - Viruses, Worms, Trojan Horses, and Time Bombs: Pranks, Prowess, Protection or Prosecution?* 41 (September 1989) (Program on Information Resources Policy, Harvard Center for Information Policy Research).

³⁸ See Statement of Senator Patrick Leahy, Hearing on Computer Viruses, Senate Subcommittee on Technology and the Law, Committee on the Judiciary, United States Senate, May 15, 1989.

⁴⁰ Vanessa Jo Grimm, "Hill Halves NIST Budget For Security," *Government Computer News*, October 30, 1989, at 1.

⁴¹ Peter G. Neumann, "A Glitch in Our Computer Thinking: We Create Powerful Systems with Pervasive Vulnerabilities," *The Los Angeles Times*, August 2, 1988, part II, at 7. A similar view was expressed by Professor Pamela Samuelson:

Probably more important than new laws or criminal prosecutions in deterring hackers from virus-related conduct would be a stronger and more effective ethical code among computer professionals and better internal policies at private firms, universities, and government institutions to regulate usage of computing resources. If hackers cannot win the admiration of their colleagues when they succeed at their clever stunts, they may be less likely to do them in the first place. And if owners of computer facilities make clear (and vigorously enforce) rules about what is acceptable and unacceptable conduct when using the system, this too may cut down on the incidence of virus experiments.

"Can Hackers Be Sued for Damages Caused by Computer Viruses?" 32 *Communications of the ACM* 666, 668-69 (June 1989).

⁴² The heads of many top U.S. computer companies could probably have been classified as "hackers" in their younger days. See generally Steven Levy, *Hackers* (1984). In fact, the chief scientist at the National Security Agency was

one of the early pioneers of Core Wars, the precursor to today's computer "virus." There has already been discussion within the computer community about how to redirect the energies of hackers toward socially beneficial goals. See, e.g., John A.N. Lee, Gerald Segal, Rosalie Steier, "Positive Alternatives: A Report on an ACM Panel on Hacking," 29 *Communications of the ACM* 297 (April 1986).

⁴³ Other countries are also confronting the question of whether to develop new laws for computer crime. In Great Britain at least one journal has questioned the wisdom of rushing forward with new legislation. "Halting Hackers," *The Economist*, October 28, 1989, at 18 ("Laws that try to make unenforceable distinctions between computer crime and ordinary crime are neither fair nor comprehensible.").