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 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-

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

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 been 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 Oversights 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 data-bases, 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 it if 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 of a valuable resource. Computer users, like users of a library, must increasingly under-stand 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 foreward 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.[32] 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."[33] 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.[34] 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.[35]

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.[36] Although computer security experts have said that such programs are potentially as dangerous as the disease they are designed to cure,[37] 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.[38]

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.[39] 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.[40] 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 short-sighted 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.[41]

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.[42] 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.[43]

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 Schmeridewaind, "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," 7 *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 part 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 krvw@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 Superintenent of Documents, Washington, DC 20402-9325 (stock number 003-003-02955-6). See also Stanley A. Kurzban, "Viruses and Worms — What Can you Do?" 7 *ACMSIG 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 described 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, 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 *CPSR 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 devices. 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 Prosection?* 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 J. 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).

[31] A compelling argument for the need to avoid restrictions on electronic communication can be found in Ithiel de Sola Pool, *Technologies of Freedom* (1983).

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

[33] 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.

[34] 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).

[35] See Wayne R. LaFave and Austin W. Scott, Jr., *Criminal Law* 5-6 (1972).

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

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

[38] 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).

[39] 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 foreward with new legislation. "Halting Hackers," *The Economist*, October 28, 1989, at 18 ("Laws that try to make untenable distinctions between computer crime and ordinary crime are neither fair nor comprehensible.").