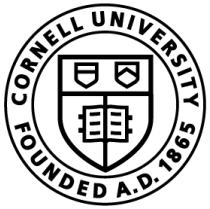


Cornell Bowers C·IS
College of Computing
and Information Science

"We have met the enemy and it is us":

Debating the ethics of computing in the pages of *CACM*

A. Feder Cooper, Solon Barocas, Karen Levy, and Gili Vidan

"We have met the enemy and it is us"

Communications of the ACM, June 1989

"We have met the enemy and it is us"

Looking at how a field of ethics can come about
in response to a particular event…

…through the response to the Morris Worm (in the *CACM* issue)

A (very) brief history of the ~~Cornell~~ Morris Worm

Cornell CHRONICLE

Volume 20 Number 12 November 10, 1988

First teaching hotel

5 Health care benefits

8 Handling hazardous chemicals

Provost orders 'virus' investigation

Provost Robert Barker has ordered an investigation into the apparent use of Cornell computers to construct a "virus" that infiltrated computers nationwide last week.

The virus, which caused thousands of computers to malfunction and slowed many business on computer networks, has been described by press reports in a first-year Cornell computer science graduate student, Robert T. Morris.

When Cornell officials examined computer files on Morris' account, they discovered lists of passwords dating from late October that were substantially similar to lists contained in the virus.

On Monday, Barker wrote a letter to M. Stuart Lynn, vice president for information technologies, asking him to head an investigative commission.

So far, the investigation "has determined that no one at Cornell in a position of responsibility authorized or had knowledge of the project that led to the creation of the virus," Barker wrote.

The university will release the results of the investigation when it is complete, "subject to appropriate legal requirements," the provost continued, and he directed that further details of the investigation not be discussed publicly until that release.

According to Lynn, his inquiry will be aided by faculty from the Department of Computer Science and from outside the department, as well as by a representative from the Office of the University Counsel.

The group will gather all evidence on Morris' potential involvement and whether other members of the Cornell community

Continued on page 12

Jill Patterson

Dean Krafft, manager of computing facilities for the computer science department, examines computer tapes containing past files from the department's computers. University investigators are examining such tapes to understand the history of the computer virus that was apparently constructed at Cornell.

Nationwide computer virus infected Cornell, too

The widely reported computer virus that infected computer systems nationwide last week also entered Cornell computers on Nov. 3, but engineers and technicians acted quickly to quash it. The Cornell supercomputers were not affected, and no permanent damage was done.

A computer virus is a program that perpetuates itself from computer to computer, sometimes doing such damage as erasing files. It propagates itself either by "infecting" computer disks that are transferred among computers or by transmitting itself over computer networks.

The virus entered Cornell through the Internet computer network, a national high-speed network connected to some 550 organizations, involving about 60,000 computers of all types. It entered thousands of other university and government laboratory computers across the country the same way. Overall, approximately 100 Cornell computers were affected by the virus.

According to Scott Brim, manager of the networking program for the Theory Center, the virus first became apparent early Thursday morning, when several computers "crashed" for no apparent reason.

When a computer system crashes, its basic operating program ceases to function, and it has to restart itself. According to Brim, the only problems presented by the virus appeared to be the periodic crashes and the slowdown of computer networks on campus because the virus was transmitting multitudes of copies of itself.

The virus infects only Digital Equipment Corp. VAXes running Berkeley UNIX as an operating system, and Sun Microsystems, Inc. workstations running OS 3 or OS 4 operating systems. The Cornell IBM supercomputers, which do not run UNIX, were not affected. The supercomputers were disconnected from the national networks for only about 30 minutes, while technicians made sure they weren't affected.

When Cornell technicians discovered that the virus was pervasive throughout Cornell, about 9:30 a.m. on Thursday, the system operators immediately disconnected Cornell from Internet and also disconnected all of Cornell's internal networks from one another to halt spread of the virus.

The system operators then began to communicate with one another to eliminate the virus. The solution was to alter the programming of the computers to protect against the virus.

"It was extremely impressive how the various departments of Cornell worked with one another," said Brim. For instance, he said, the electrical engineering department and the Theory Center obtained the program fixes for VAXes from sources outside Cornell, and the Laboratory for Solid State Physics developed program fixes for SUN workstations. Also, the Laboratory for Plasma studies developed program fixes for Ultrix — the DEC version of UNIX — and the computer science department analyzed the behavior of the virus.

By Thursday evening, almost all the Cornell networks had been reconnected with one another.

Specifically, the virus was carried through the electronic mail system that runs on Berkeley UNIX and its derivatives. It took advantage of weaknesses in the computer code that receives mail to be sent, and also in weaknesses in a small program called Finger Daemon that allows users to find out who is using a computer and where they are on the system. The virus also propagated itself from machine to machine

Virus' investigation continued from page 1

were either involved in or aware of the potential virus attack, he said.

He also hopes to determine which Cornell computer policies, if any, were violated in the incident and whether any should be modified to prevent security violations. No timetable has been set for the report.

The university is in contact with federal and state authorities. The FBI is responsible for the federal criminal investigation of the incident. As of yesterday morning, university officials had not yet talked to Morris.

As a routine security measure, the university has closed Morris' computer account. All computer tapes and other materials have been copied, with the originals under strict security.

"Some have characterized the creation of this virus as the work of a folk hero," Barker wrote. "Others have indicated that some positive results may occur as a result of increased attention to computer and network security. Still others have speculated that the damage was an unintended result of what was originally designed to be a benign

by taking advantage of a feature called "equivalency" in which machines are defined to be the same for ease of access by various users. The virus also took advantage of a feature in which users could specify themselves to have equal rights to various machines.

—Dennis Meredith

experiment. Cornell takes a very different view and thoroughly deplores any action that disrupts or put at risk computer systems or networks here or elsewhere.

"Such irresponsible behavior violates the most fundamental principles of ethical behavior. Those found in violation of university rules and regulations involving such behavior will be subject to appropriate disciplinary action," Barker wrote.

On Wednesday, the faculty of the computer science department also passed a resolution denouncing the release of the virus:

"Computer scientists are fully aware that computers are easily misused with potentially catastrophic consequences. As such we have a special duty to exercise and promote the highest sense of responsibility and the most exacting standard of ethical behavior. We insist that the members of the department use all equipment with care and responsibility. We shall do everything possible to prevent a repetition of the deplorable incidents of last week."

—Dennis Meredi

The Cornell Commission: On Morris and the Worm

After careful examination of the evidence, the Cornell commission publishes its findings in a detailed report that sheds new light and dispels some myths about Robert T. Morris and the Internet worm.

Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro

Cornell Information Technologies records, Kroch Library, Box 60, Folder C

A (very) brief history of the ~~Cornell~~ Morris Worm

Cornell CHRONICLE

Volume 20 Number 12 November 10, 1988

First teaching hotel

5 Health care benefits

8 Handling hazardous chemicals

Provost orders 'virus' investigation

Provost Robert Barker has ordered an investigation into the apparent use of Cornell computers to construct a "virus" that infiltrated computers nationwide last week.

The virus, which caused thousands of computers to malfunction and slowed many machines on computer networks, has been described by press reports in a first-year Cornell computer science graduate student, Robert T. Morris.

When Cornell officials examined computer files on Morris' account, they discovered lists of passwords dating from late October that were substantially similar to lists contained in the virus.

On Monday, Barker wrote a letter to M. Stuart Lynn, vice president for information technologies, asking him to head an investigative commission.

So far, the investigation "has determined that no one at Cornell in a position of responsibility authorized or had knowledge of the project that led to the creation of the virus," Barker wrote.

The university will release the results of the investigation when it is complete, "subject to appropriate legal requirements," the provost continued, and he directed that further details of the investigation not be disclosed publicly until that release.

According to Lynn, his inquiry will be aided by faculty from the Department of Computer Science and from outside the department, as well as by a representative from the Office of the University Counsel.

The group will gather all evidence on Morris' potential involvement and whether other members of the Cornell community

Continued on page 12

Jill Fehrenbacher

Dean Krafft, manager of computing facilities for the computer science department, examines computer tapes containing past files from the department's computers. University investigators are examining such tapes to understand the history of the computer virus that was apparently constructed at Cornell.

Nationwide computer virus infected Cornell, too

The widely reported computer virus that infected computer systems nationwide last week also entered Cornell computers on Nov. 3, but engineers and technicians acted quickly to quash it. The Cornell supercomputers were not affected, and no permanent damage was done.

A computer virus is a program that perpetuates itself from computer to computer, sometimes doing such damage as erasing files. It propagates itself either by "infecting" computer disks that are transferred among computers or by transmitting itself over computer networks.

The virus entered Cornell through the Internet computer network, a national high-speed network connected to some 550 organizations, involving about 60,000 computers of all types. It entered thousands of other university and government laboratory computers across the country the same way. Overall, approximately 100 Cornell computers were affected by the virus.

According to Scott Brim, manager of the networking program for the Theory Center, the virus first became apparent early Thursday morning, when several computers "crashed" for no apparent reason.

When a computer system crashes, its basic operating program ceases to function, and it has to restart itself. According to Brim, the only problems presented by the virus appeared to be the periodic crashes and the slowdown of computer networks on campus because the virus was transmitting multitudes of copies of itself.

The virus infects only Digital Equipment Corp. VAXes running Berkeley UNIX as an operating system, and Sun Microsystems, Inc. workstations running OS 3 or OS 4 operating systems. The Cornell IBM supercomputers, which do not run UNIX, were not affected. The supercomputers were disconnected from the national networks for only about 30 minutes, while technicians made sure they weren't affected.

When Cornell technicians discovered that the virus was pervasive throughout Cornell, about 9:30 a.m. on Thursday, the system operators immediately disconnected Cornell from Internet and also disconnected all of Cornell's internal networks from one another to halt spread of the virus.

The system operators then began to communicate with one another to eliminate the virus. The solution was to alter the programming of the computers to protect against the virus.

"It was extremely impressive how the various departments of Cornell worked with one another," said Brim. For instance, he said, the electrical engineering department and the Theory Center obtained the program fixes for VAXes from sources outside Cornell, and the Laboratory for Solid State Physics developed program fixes for SUN workstations. Also, the Laboratory for Plasma studies developed program fixes for Ultrix — the DEC version of UNIX — and the computer science department analyzed the behavior of the virus.

By Thursday evening, almost all the Cornell networks had been reconnected with one another.

Specifically, the virus was carried through the electronic mail system that runs on Berkeley UNIX and its derivatives. It took advantage of weaknesses in the computer code that receives mail to be sent, and also in weaknesses in a small program called Finger Daemon that allows users to find out who is using a computer and where they are on the system. The virus also propagated itself from machine to machine by taking advantage of a feature called "equivalency" in which machines are defined to be the same for ease of access by various users. The virus also took advantage of a feature in which users could specify themselves to have equal rights to various machines.

—Dennis Meredith

Virus' investigation continued from page 1

were either involved in or aware of the potential virus attack, he said.

He also hopes to determine which Cornell computer policies, if any, were violated in the incident and whether any should be modified to prevent security violations. No timetable has been set for the report.

The university is in contact with federal and state authorities. The FBI is responsible for the federal criminal investigation of the incident. As of yesterday morning, university officials had not yet talked to Morris.

As a routine security measure, the university has closed Morris' computer account. All computer tapes and other relevant materials have been copied, with the originals under strict security.

"Some have characterized the creation of this virus as the work of a folk hero," Barker wrote. "Others have indicated that some positive results may occur as a result of increased attention to computer and network security. Still others have speculated that the damage was an unintended result of what was originally designed to be a benign experiment. Cornell takes a very different view and thoroughly deplores any actions that disrupt or put at risk computer systems or networks here or elsewhere.

"Such irresponsible behavior violates the most fundamental principles of ethical behavior. Those found in violation of university rules and regulations involving such behavior will be subject to appropriate disciplinary action," Barker wrote.

On Wednesday, the faculty of the computer science department also passed a resolution denouncing the release of the virus:

"Computer scientists are fully aware that computers are easily misused with potentially catastrophic consequences. As such we have a special duty to exercise and promote the highest sense of responsibility as the most exacting standard of ethical behavior. We insist that the members of the department use all equipment with care and responsibility. We shall do everything possible to prevent a repetition of the deplorable incidents of last week."

—Dennis Meredith

The Cornell Commission: On Morris and the Worm

After careful examination of the evidence, the Cornell commission publishes its findings in a detailed report that sheds new light and dispels some myths about Robert T. Morris and the Internet worm.

Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro

10. Security Considerations RFC 1135

If security considerations had not been so widely ignored in the Internet, this memo would not have been possible.

Cornell Information Technologies records, Kroch Library, Box 60, Folder C

A (very) brief history of the ~~Cornell~~ Morris Worm

Cornell CHRONICLE

First teaching hotel

5 Health care benefits

8 Handling hazardous chemicals

Volume 20 Number 12 November 10, 1988

Provost orders 'virus' investigation

Provost Robert Barker has ordered an investigation into the apparent use of Cornell computers to construct a "virus" that infiltrated computers nationwide last week.

The virus, which caused thousands of computers to malfunction and slowed transmissions on computer networks, has been linked by press reports to a first-year Cornell computer science graduate student, Robert T. Morris.

When Cornell officials examined computer files on Morris' account, they discovered lists of passwords dating from late October that were substantially similar to lists contained in the virus.

On Monday, Barker wrote a letter to M. Stuart Lynn, vice president for information technologies, asking him to head an investigative commission.

So far, the investigation "has determined that no one at Cornell in a position of responsibility authorized or had knowledge of the project that led to the creation of the virus," Barker wrote.

The university will release the results of the investigation when it is complete, "subject to appropriate legal requirements," the provost continued, and he directed that further details of the investigation not be discussed publicly until that release.

According to Lynn, his inquiry will be aided by faculty from the Department of Computer Science and from outside the department, as well as by a representative from the Office of the University Counsel.

The group will gather all evidence on Morris' potential involvement and whether other members of the Cornell community

Continued on page 12

Jill Peltzman

Dean Krafft, manager of computing facilities for the computer science department, examines computer tapes containing past files from the department's computers. University investigators are examining such tapes to understand the history of the computer virus that was apparently constructed at Cornell.

Nationwide computer virus infected Cornell, too

The widely reported computer virus that infected computer systems nationwide last week also entered Cornell computers on Nov. 3, but engineers and technicians acted quickly to quash it. The Cornell supercomputers were not affected, and no permanent damage was done.

A computer virus is a program that perpetuates itself from computer to computer, sometimes doing such damage as erasing files. It propagates itself either by "infecting" computer disks that are transfered among computers or by transmitting itself over computer networks.

The virus entered Cornell through the Internet computer network, a national high-speed network connected to some 550 organizations, involving about 60,000 computers of all types. It entered thousands of other university and government laboratory computers across the country the same way. Overall, approximately 100 Cornell computers were affected by the virus.

According to Scott Brim, manager of the networking program for the Theory Center, the virus first became apparent early Thursday morning, when several computers "crashed" for no apparent reason.

When a computer system crashes, its basic operating program ceases to function, and it has to restart itself. According to Brim, the only problems presented by the virus appeared to be the periodic crashes and the slowdown of computer networks on campus because the virus was transmitting multitudes of copies of itself.

The virus infects only Digital Equipment Corp. VAXes running Berkeley UNIX as an operating system, and Sun Microsystems, Inc. workstations running OS 3 or OS 4 operating systems. The Cornell IBM supercomputers, which do not run UNIX, were not affected. The supercomputers were disconnected from the national networks for only about 30 minutes, while technicians made sure they weren't affected.

When Cornell technicians discovered that the virus was pervasive throughout Cornell, about 9:30 a.m. on Thursday, the system operators immediately disconnected Cornell from Internet and also disconnected all of Cornell's internal networks from one another to halt spread of the virus.

The system operators then began to communicate with one another to eliminate the virus. The solution was to alter the programming of the computers to protect agains the virus.

"It was extremely impressive how the various departments of Cornell worked with one another," said Brim. For instance, he said, the electrical engineering department and the Theory Center obtained the program fixes for VAXes from sources outside Cornell, and the Laboratory for Solid State Physics developed program fixes for SUN workstations. Also, the Laboratory for Plasma studies developed program fixes for Ultrix — the DEC version of UNIX — and the computer science department analyzed the behavior of the virus.

By Thursday evening, almost all the Cornell networks had been reconnected with one another.

Specifically, the virus was carried through the electronic mail system that runs on Berkeley UNIX and its derivatives. It took advantage of weaknesses in the computer code that receives mail to be sent, and also in weaknesses in a small program called Finger Daemon that allows users to find out who is using a computer and where they are on the system. The virus also propagated itself from machine to machine by taking advantage of a feature called "equivalency" in which machines are defined to be the same for ease of access by various users. The virus also took advantage of a feature in which users could specify themselves to have equal rights to various machines.

—*Dennis Meredith*

'Virus' investigation *continued from page 1*

were either involved in or aware of the potential virus attack, he said.

He also hopes to determine which Cornell computer policies, if any, were violated in the incident and whether any should be modified to prevent security violations. No timetable has been set for the report .

The university is in contact with federal and state authorities. The FBI is responsible for the federal criminal investigation of the incident. As of yesterday morning, university officials had not yet talked to Morris.

As a routine security measure, the university has closed Morris' computer account. All computer tapes and other relevant materials have been copied, with the originals under strict security.

"Some have characterized the creation of this virus as the work of a folk hero," Barker wrote. "Others have indicated that some positive results may occur as a result of increased attention to computer and network security. Still others have speculated that the damage was an unintended result of what was originally designed to be a benign experiment. Cornell takes a very different view and thoroughly deplores any actions that disrupt or put at risk computer systems or networks here or elsewhere.

"Such irresponsible behavior violates the most fundamental principles of ethical behavior. Those found in violation of university rules and regulations involving such behavior will be subject to appropriate disciplinary action," Barker wrote.

On Wednesday, the faculty of the computer science department also passed a resolution denouncing the release of the virus:

"Computer scientists are fully aware that computers are easily misused with potentially catastrophic consequences. As such we have a special duty to exercise and promote the highest sense of responsibility and the most exacting standard of ethical behavior. We insist that the members of the department use all equipment with care and responsibility. We shall do everything possible to prevent a repetition of the deplorable incidents of last week."

—*Dennis Meredith*

Cornell Information Technologies records, Kroch Library, Box 60, Folder C

The Cornell Commission: On Morris and the Worm

After careful examination of the evidence, the Cornell commission publishes its findings in a detailed report that sheds new light and dispels some myths about Robert T. Morris and the Internet worm.

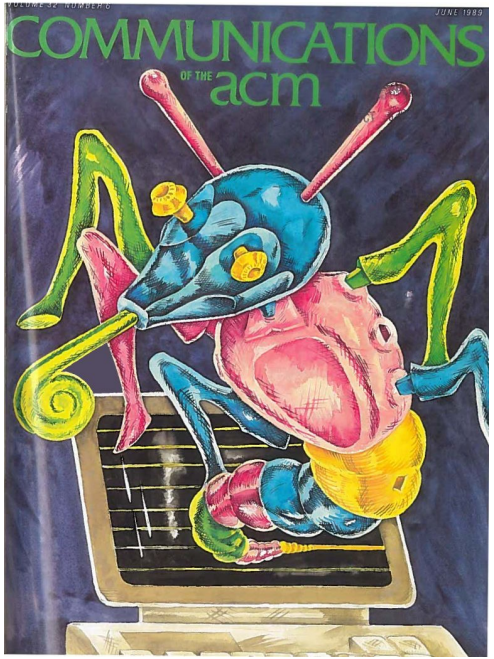
Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro

10. Security Considerations RFC 1135

```
If security considerations had not been so widely ignored in the
Internet, this memo would not have been possible.
```

"We have met the enemy and it is us"

The *CACM* Special Issue

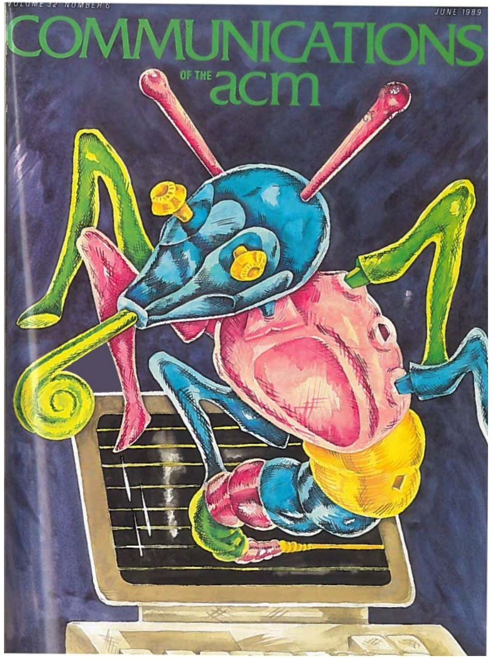


The Cornell Commission: On Morris and the Worm

After careful examination of the evidence, the Cornell commission publishes its findings in a detailed report that sheds new light and dispels some myths about Robert T. Morris and the Internet worm.

Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro

The *CACM* Special Issue



Ethics and the Internet

At great human and economic cost, resources drawn from the U.S. government, industry and the academic community have been assembled into a collection of interconnected networks called the Internet. Begun as a vehicle for experimental network research in the mid-1970s, the Internet has become an important national infrastructure supporting an increasingly widespread, multi-disciplinary community of researchers ranging, inter alia, from computer scientists and electrical engineers to mathematicians, physicists, medical researchers, chemists, astronomers and space scientists.

STATEMENT OF ETHICS

As is true of other common infrastructures (e.g., roads, water reservoirs and delivery systems, and the power generation and distribution network), there is widespread dependence on the Internet by its users for the support of day-to-day research activities.

The reliable operation of the Internet and the responsible use of its resources is of common interest and concern for its users, operators, and sponsors. Recent events involving the hosts on the Internet and in similar network infrastructures underscore the need to reiterate the professional responsibility every Internet user bears to colleagues and to the sponsors of the system. Many of the Internet resources are provided by the U.S. Government. Abuse of the system thus becomes a federal matter above and beyond simple professional ethics.

Statement of Policy

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. government—sponsors of this system—suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The Internet Activities Board (IAB) strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

a. seeks to gain unauthorized access to the resources of the Internet,
b. disrupts the intended use of the Internet,
c. wastes resources (people, capacity, computer) through such actions,
d. destroys the integrity of computer-based information, and/or
e. compromises the privacy of users.

The Internet exists in the general research milieu. Portions of it continue to be used to support research and experimentation on networking. Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise great caution in the conduct of their work. Negligence in the conduct on Internet-wide experiments is both irresponsible and unacceptable.

The IAB plans to take whatever actions it can, in concert with Fed-

CPSR Statement on the Computer Virus

The so-called computer virus that swept through a national computer network, the Internet, in early November (1988) is a dramatic example of the vulnerability of complex computer systems. It temporarily denied service to thousands of computer users at academic, business, and military sites. An estimated 6,000 computers across the country were affected in only a few hours. Fortunately, the program was not designed to delete or alter data—the impact of a malicious virus would have been immeasurable.

This was an irresponsible act that cannot be condoned. The Internet should not be treated as a laboratory for uncontrolled experiments in computer security. Networked software is intrinsically risky, and no programmer can guarantee that a self-replicating program will not have unintended consequences.

STATEMENT OF ETHICS

The value of open networks depends upon the good will and good sense of computer users. Computer professionals should take upon themselves the responsibility to ensure that systems are not misused. Individual accountability is all the more important when people work together through a network of shared resources. Computer professionals should establish and encourage ethics based on the shared needs of network users. We also encourage educators to teach these ethics.

The questions of legal responsibility in this instance are ultimately for our legal system to resolve. The questions confronting computer professionals and others concerned about the future of our technology policy go well beyond this particular case. The incident underscores our society's increasing dependence on complex computer networks. Security flaws in networks, in computer operating systems, and in management practices have been amply demonstrated by break-ins at Stanford University, by the penetration of national research networks, and by the "Christmas virus" that clogged the IBM internal network last December.

Computer Professionals for Social Responsibility (CPSR) believes that this incident should prompt critical review of our dependence on complex computer networks, particularly for military and defense-related

widely accessible.

An effective way to correct known security flaws is to publish descriptions of the flaws so that they can be corrected. We therefore view the efforts to conceal technical descriptions of the recent virus as short-sighted.

CPSR believes that innovation, creativity and the open exchange of ideas are the ingredients of scientific advancement and technological achievement. Computer networks, such as the Internet, facilitate this exchange. We cannot afford policies that might restrict the ability of computer researchers to exchange their ideas with one another. More secure networks, such as military and financial networks, sharply restrict access and offer limited functionality. Government, industry, and the university community should support the continued development of network technology that provides open access to many users.

The computer virus has sent a clear warning to the computing community and to society at large. We hope it will provoke a long overdue public discussion about the vul-

Teaching Students About Responsible Use of

There has been some discussion in *Risks Forum* recently about what action universities might appropriately take to instill a sense of ethics in the use of computers by their students. M.I.T.'s Project Athena provides some 800 networked engineering workstations for undergraduates to use in any way they find helpful to their education. Accordingly, Project Athena has assumed that one of its responsibilities is to open a discussion of ethical use with its user community. The primary action that Project Athena has taken is the publication of a set of principles.

These principles are general, for the most part, following M.I.T.'s usual approach of appealing to basic concepts rather than spelling out many detailed rules. There is no claim that publicizing these principles completely solves any problem nor that it completely answers any question, but it does represent one organization's attempt to take a step in the right direction. Some version of these principles have been posted for about four years, and whenever we have an incident serious enough to ask a student to talk to the director, these principles have provided a useful starting point for the conversation.

STATEMENT OF ETHICS

Principles of Responsible Use of Project Athena

Project Athena is M.I.T.'s computing facility for education. It consists of a networked system of workstations and services, and includes communication features that offer many opportunities for members of the M.I.T. community to share information.

With that ability to share comes the responsibility to use the system in accordance with M.I.T.'s standards of honesty and personal conduct. Those standards, outlined in the M.I.T. Bulletin under academic procedures, call for all members of the community to act in a responsible, ethical and professional way. What follows are guidelines in applying those standards to use of Project Athena facilities.

Intended Use

The hardware granted to Project Athena, and the software licensed for that hardware, are intended for educational use, broadly construed, by members of the M.I.T. community. Use of Athena resources by anyone outside M.I.T. requires approval of the provost, and the sale of such use is improper. The use of Project Athena's facilities for sponsored research activities that normally would make use of other M.I.T. facilities requires specific authorization of the director.

Privacy and Security

The operating systems used by Project Athena encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing. Users must supplement the system's security mechanisms by using the system in a manner that preserves the privacy of others.

For example, users should not attempt to gain access to the files or directories of another user without clear authorization from the other user (typically that authorization is

tions, attempts to capture or crack passwords or encryption, and destruction or alteration of data or programs belonging to other users. Equally unacceptable are intentional efforts to restrict or deny access by legitimate users to the system.

Intellectual Property Rights

Some software and data that reside on the system are owned by users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. Users must abide by these restrictions. Such restrictions may include prohibitions against copying programs or data for use on non-Athena systems or for distribution outside M.I.T., against the resale of data or programs or the use of them for noneducational purposes or for financial gain, and against public disclosure of information about programs (e.g., source code) without the owner's authorization. It is the responsibility of the owner of protected software or data to make any such restrictions known to the user. □

Jerome H. Saltzer
Athena Project, M.I.T.

NSF Poses Code of Networking Ethics

The network worm (sometimes called virus) affair raises issues that are very important to our field. Both the BITNET Board of Trustees and the CSNET Executive Committee have been struck by the fact that many public comments on the event have contained statements such as:

"We learned from it."

"We will make sure technically it will not happen again."

"He did us a favor by showing…" unaccompanied by expressions of ethical concern.

As a profession we have succeeded technically in creating facilities—the BITNET, CSNET and other components of the national research network—which are now critical to the conduct of science and engineering in our nation's academic, industrial, and government research laboratories. Further, this technology has spread within our nation's commercial research and development organizations and even into their manufacturing and marketing.

STATEMENT OF ETHICS

Just as medical malpractice can have a serious effect on an individual's health, one of the costs of our success is that we are now in a position where misuse of our national and private computer networks can have as serious an effect on the nation's economic, defense, and social health. Yet while almost every medical college has at least one course on medical ethics and insists on the observance of ethical guidelines during practice, computer scientists seem to avoid such non-scientific issues.

The worm *experiment* caused a major disruption in the research community. Among other points of attack, the worm exploited a trapdoor that has been distributed as a software *feature*. Many hours of talent were wasted finding and curing the problems raised by this *game*. Many additional hours were lost when researchers were unable to access supercomputers and mail systems due to system overload and network shutdown.

We condemn the perpetration of such experiments, games, or features by workers in our field, be they students, faculty, researchers or providers. We are especially worried about widespread tendencies to justify, ignore, or perpetuate such breaches. We must behave as do our fellow scientists who have organized around comparable issues to enforce strong ethical practices in the conduct of experiments.

We propose to join with the relevant professional societies and the national research networks to form a Joint Ethics Committee charged with examining existing statements of professional ethics and modifying them as necessary in order to create a strong statement of networking ethics and recommendations for appropriate enforcement procedures.

In its biannual meeting last December the Division Advisory Panel (DAP) of the National Science Foundation (NSF) Division of Networking and Communications Research and Infrastructure (DNCRI) resolved to unanimously support the statement of BITNET/CSNET on the breach of ethics implied by the worm. The group also unanimously endorsed the following statement:

Ethical Network Use Statement

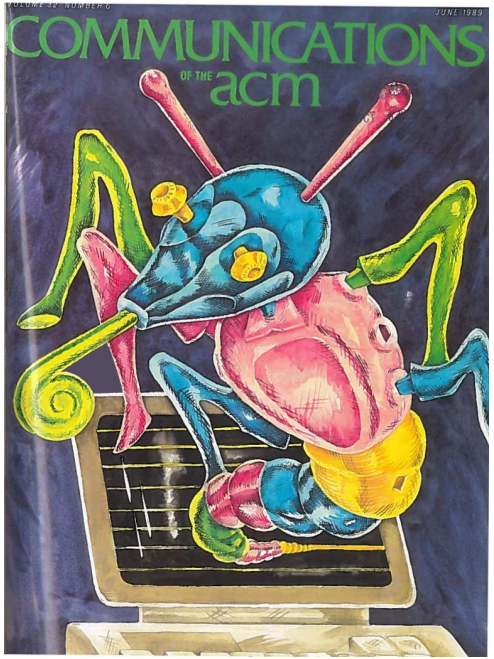
The DAP of the NSF DNCRI deplores lapses of ethical behavior which cause disruption to our national network resources. Industry, government and academe have established computer networks in support of research and scholarship. Recent events have accentuated the importance of establishing community standards for the ethical use of networks. In this regard, the DNCRI DAP defines as unethical any activity which purposefully or through negligence:

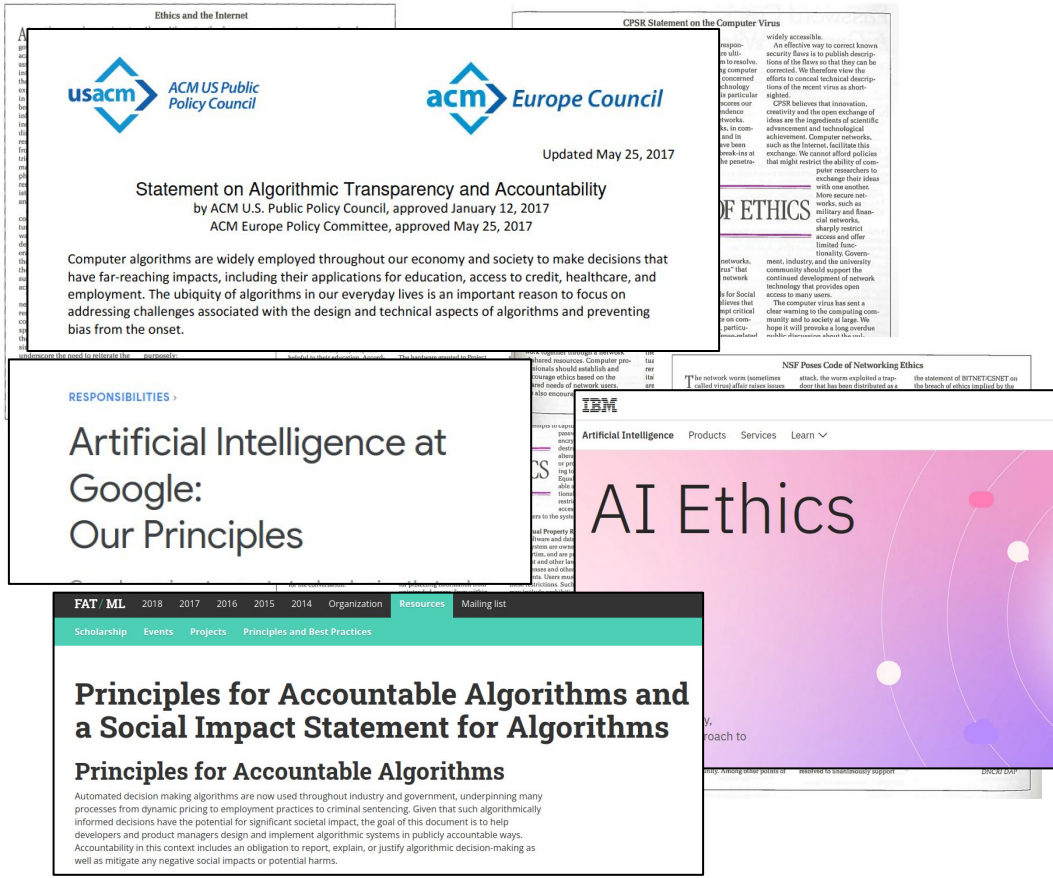
a. disrupts the intended use of the networks
b. wastes resources through such actions (people, bandwidth or computer)
c. destroys the integrity of computer-based information
d. compromises the privacy of users
e. consumes unplanned resources for control and eradication.

We encourage organizations managing and operating networks to adopt and publicize policies and standards for ethical behavior. We also encourage these organizations to adopt administrative procedures to enforce appropriate disciplinary responses to violations and to work with appropriate bodies on drafting legislation in this area. □

David J. Farber
Chair
DNCRI DAP

The *CACM* Special Issue





The *CACM* Issue Ethics Statements

Ethics and the Internet

STATEMENT OF ETHICS

A t great human and economic cost, resources drawn from the U.S. government, industry and the academic community have been assembled into a collection of interconnected networks called the Internet. Begun as a vehicle for experimental network research in the mid-1970s, the Internet has become an important national infrastructure supporting an increasingly widespread, multi-disciplinary community of researchers ranging, inter alia, from computer scientists and electrical engineers to mathematicians, physicists, medical researchers, chemists, astronomers and space scientists.

As is true of other common infrastructures (e.g., roads, water reservoirs and delivery systems, and the power generation and distribution network), there is widespread dependence on the Internet by its users for the support of day-to-day research activities.

The reliable operation of the Internet and the responsible use of its resources is of common interest and concern for its users, operators, and sponsors. Recent events involving the hosts on the Internet and in similar network infrastructures underscore the need to reiterate the professional responsibility every Internet user bears to colleagues and to the sponsors of the system. Many of the Internet resources are provided by the U.S. Government. Abuse of the system thus becomes a federal matter above and beyond simple professional ethics.

Statement of Policy

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. government—sponsors of this system—suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The Internet Activities Board (IAB) strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

a. seeks to gain unauthorized access to the resources of the Internet,
b. disrupts the intended use of the Internet,
c. wastes resources (people, capacity, computer) through such actions,
d. destroys the integrity of computer-based information, and/or
e. compromises the privacy of users.

The Internet exists in the general research milieu. Portions of it continue to be used to support research and experimentation on networking. Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise great caution in the conduct of their work. Negligence in the conduct on Internet-wide experiments is both irresponsible and unacceptable.

The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up technical and procedural mechanisms to make the Internet more resistant to disruption. Such security, however, may be extremely expensive and may be counterproductive if it inhibits the free flow of information which makes the Internet so valuable. In the final analysis, the health and well-being of the Internet is the responsibility of its users who must, uniformly, guard against abuses which disrupt the system and threatens its long-term viability. □

Vint Cerf
Internet Activities Board

Teaching Students About Responsible Use of Computers

STATEMENT OF ETHICS

There has been some discussion in *Risks Forum* recently about what action universities might appropriately take to instill a sense of ethics in the use of computers by their students. M.I.T.'s Project Athena provides some 800 networked engineering workstations for undergraduates to use in any way they find helpful to their education. Accordingly, Project Athena has assumed that one of its responsibilities is to open a discussion of ethical use with its user community. The primary action that Project Athena has taken is the publication of a set of principles.

These principles are general, for the most part, following M.I.T.'s usual approach of appealing to basic concepts rather than spelling out many detailed rules. There is no claim that publicizing these principles completely solves any problem nor that it completely answers any question, but it does represent one organization's attempt to take a step in the right direction. Some version of these principles have been posted for about four years, and whenever we have an incident serious enough to ask a student to talk to the director, these principles have provided a useful starting point for the conversation.

Principles of Responsible Use of Project Athena

Project Athena is M.I.T's computing facility for education. It consists of a networked system of workstations and services, and includes communication features that offer many opportunities for members of the M.I.T. community to share information.

With that ability to share comes the responsibility to use the system in accordance with M.I.T's standards of honesty and personal conduct. Those standards, outlined in the M.I.T. Bulletin under academic procedures, call for all members of the community to act in a responsible, ethical and professional way. What follows are guidelines in applying those standards to use of Project Athena facilities.

Intended Use

The hardware granted to Project Athena, and the software licensed for that hardware, are intended for educational use, broadly construed, by members of the M.I.T. community. Use of Athena resources by anyone outside M.I.T. requires approval of the provost, and the sale of such use is improper. The use of Project Athena's facilities for sponsored research activities that normally would make use of other M.I.T. facilities requires specific authorization of the director.

Privacy and Security

The operating systems used by Project Athena encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing. Users must supplement the system's security mechanisms by using the system in a manner that preserves the privacy of others.

For example, users should not attempt to gain access to the files or directories of another user without clear authorization from the other user (typically that authorization is expressed by setting file access permissions to allow public or group reading). Nor should users attempt to intercept any network communications, such as electronic mail or user-to-user dialog. A shared program should not be stored or communicated on the systems. Examples of such personal information are grades or letters of recommendation.

System Integrity

Actions taken by users intentionally to interfere with or to alter the integrity of the system are out of bounds. Such actions include unauthorized use of accounts, impersonation of other individuals in communications, attempts to capture or crack passwords or encryption, and destruction or alteration of data or programs belonging to other users. Equally unacceptable are intentional efforts to restrict or deny access by legitimate users to the system.

Intellectual Property Rights

Some software and data that reside on the system are owned by users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. Users must abide by these restrictions. Such restrictions may include prohibitions against copying programs or data for use on non-Athena systems or for distribution outside M.I.T., against the resale of data or programs or the use of them for noneducational purposes or for financial gain, and against public disclosure of information about programs (e.g., source code) without the owner's authorization. It is the responsibility of the owner of protected software or data to make any such restrictions known to the user. □

Jerome H. Saltzer
Athena Project, M.I.T.

CPSR Statement on the Computer Virus

STATEMENT OF ETHICS

The so-called computer virus that swept through a national computer network, the Internet, in early November (1988) is a dramatic example of the vulnerability of complex computer systems. It temporarily denied service to thousands of computer users at academic, business, and military sites. An estimated 6,000 computers across the country were affected in only a few hours. Fortunately, the program was not designed to delete or alter data—the impact of a malicious virus would have been immeasurable.

This was an irresponsible act that cannot be condoned. The Internet should not be treated as a laboratory for uncontrolled experiments in computer security. Networked software is intrinsically risky, and no programmer can guarantee that a self-replicating program will not have unintended consequences.

The value of open networks depends upon the good will and good sense of computer users. Computer professionals should take upon themselves the responsibility to ensure that systems are not misused. Individual accountability is all the more important when people work together through a network of shared resources. Computer professionals should establish and encourage ethics based on the shared needs of network users. We also encourage educators to teach these ethics.

The questions of legal responsibility in this instance are ultimately for our legal system to resolve. The questions confronting computer professionals and others concerned about the future of our technology policy go well beyond this particular case. The incident underscores our society's increasing dependence on complex computer networks. Security flaws in networks, in computer operating systems, and in management practices have been amply demonstrated by break-ins at Stanford University, by the penetration of national research networks, and by the "Christmas virus" that clogged the IBM internal network last December.

Computer Professionals for Social Responsibility (CPSR) believes that this incident should prompt critical review of our dependence on complex computer networks, particularly for military and defense-related functions. The flaws that permitted the recent virus to spread will eventually be fixed, but other flaws will remain. Security loopholes are inevitable in any computer network and are prevalent in those that support general-purpose computing and are widely accessible.

An effective way to correct known security flaws is to publish descriptions of the flaws so that they can be corrected. We therefore view the efforts to conceal technical descriptions of the recent virus as short-sighted.

CPSR believes that innovation, creativity and the open exchange of ideas are the ingredients of scientific advancement and technological achievement. Computer networks, such as the Internet, facilitate this exchange. We cannot afford policies that might restrict the ability of computer researchers to exchange their ideas with one another. More secure networks, such as military and financial networks, sharply restrict access and offer limited functionality. Government, industry, and the university community should support the continued development of network technology that provides open access to many users.

The computer virus has sent a clear warning to the computing community and to society at large. We hope it will provoke a long overdue public discussion about the vulnerabilities of computer networks, and the technological, ethical and legal choices we must address. □

Gary Chapman
Executive Director
Computer Professionals for Social Responsibility

NSF Poses Code of Networking Ethics

STATEMENT OF ETHICS

The network worm (sometimes called virus) affair raises issues that are very important to our field. Both the BITNET Board of Trustees and the CSNET Executive Committee have been struck by the fact that many public comments on the event have contained statements such as:

"We learned from it."

"We will make sure technically it will not happen again."

"He did us a favor by showing..." unaccompanied by expressions of ethical concern.

As a profession we have succeeded technically in creating facilities—the BITNET, CSNET and other components of the national research network—which are now critical to the conduct of science and engineering in our nation's academic, industrial, and government research laboratories. Further, this technology has spread within our nation's commercial research and development organizations and even into their manufacturing and marketing.

Just as medical malpractice can have a serious effect on an individual's health, one of the costs of our success is that we are now in a position where misuse of our national and private computer networks can have as serious an effect on the nation's economic, defense, and social health. Yet while almost every medical college has at least one course on medical ethics and insists on the observance of ethical guidelines during practice, computer scientists seem to avoid such non-scientific issues.

The worm *experiment* caused a major disruption in the research community. Among other points of attack, the worm exploited a trapdoor that has been distributed as a software *feature*. Many hours of talent were wasted finding and curing the problems raised by this *gene*. Many additional hours were lost when researchers were unable to access supercomputers and mail systems due to system overload and network shutdown.

We condemn the perpetration of such experiments, games, or features by workers in our field, be they students, faculty, researchers or providers. We are especially worried about widespread tendencies to justify, ignore, or perpetuate such breeches. We must behave as do our fellow scientists who have organized around comparable issues to enforce strong ethical practices in the conduct of experiments.

We propose to join with the relevant professional societies and the national research networks to form a Joint Ethics Committee charged with examining existing statements of professional ethics and modifying them as necessary in order to create a strong statement of networking ethics and recommendations for appropriate enforcement procedures.

In its biannual meeting last December the Division Advisory Panel (DAP) of the National Science Foundation (NSF) Division of Networking and Communications Research and Infrastructure (DNCRI) resolved to unanimously support the statement of BITNET/CSNET on the breach of ethics implied by the worm. The group also unanimously endorsed the following statement:

Ethical Network Use Statement

The DAP of the NSF DNCRI deplores lapses of ethical behavior which cause disruption to our national network resources. Industry, government and academe have established computer networks in support of research and scholarship. Recent events have accentuated the importance of establishing community standards for the ethical use of networks. In this regard, the DNCRI DAP defines as unethical any activity which purposefully or through negligence:

a. disrupts the intended use of the networks
b. wastes resources through such actions (people, bandwidth or computer)
c. destroys the integrity of computer-based information
d. compromises the privacy of users
e. consumes unplanned resources for control and eradication.

We encourage organizations managing and operating networks to adopt and publicize policies and standards for ethical behavior. We also encourage these organizations to adopt administrative procedures to enforce appropriate disciplinary responses to violations and to work with appropriate bodies on drafting legislation in this area. □

David J. Farber
Chair
DNCRI DAP

The *CACM* Issue Ethics Statements

Ethics and the Internet

STATEMENT OF ETHICS

At great human and economic cost, resources drawn from the U.S. government, industry and the academic community have been assembled into a collection of interconnected networks called the Internet. Begun as a vehicle for experimental network research in the mid-1970s, the Internet has become an important national infrastructure supporting an increasingly widespread, multi-disciplinary community of researchers ranging, inter alia, from computer scientists and electrical engineers to mathematicians, physicists, medical researchers, chemists, astronomers and space scientists.

As is true of other common infrastructures (e.g., roads, water reservoirs and delivery systems, and the power generation and distribution network), there is widespread dependence on the Internet by its users for the support of day-to-day research activities.

The reliable operation of the Internet and the responsible use of its resources is of common interest and concern for its users, operators, and sponsors. Recent events involving the hosts on the Internet and in similar network infrastructures underscore the need to reiterate the professional responsibility every Internet user bears to colleagues and to the sponsors of the system. Many of the Internet resources are provided by the U.S. Government. Abuse of the system thus becomes a federal matter above and beyond simple professional ethics.

Statement of Policy

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. government—sponsors of this system—suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The Internet Activities Board (IAB) strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

a. seeks to gain unauthorized access to the resources of the Internet,
b. disrupts the intended use of the Internet,
c. wastes resources (people, capacity, computer) through such actions,
d. destroys the integrity of computer-based information, and/or
e. compromises the privacy of users.

The Internet exists in the general research milieu. Portions of it continue to be used to support research and experimentation on networking. Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise great caution in the conduct of their work. Negligence in the conduct on Internet-wide experiments is both irresponsible and unacceptable.

The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up technical and procedural mechanisms to make the Internet more resistant to disruption. Such security, however, may be extremely expensive and may be counterproductive if it inhibits the free flow of information which makes the Internet so valuable. In the final analysis, the health and well-being of the Internet is the responsibility of its users who must, uniformly, guard against abuses which disrupt the system and threatens its long-term viability. □

Vint Cerf
Internet Activities Board

Internet Activities Board

(RFC 1087)
January, 1989

Teaching Students About Responsible Use of Computers

STATEMENT OF ETHICS

There has been some discussion in *Risks Forum* recently about what action universities might appropriately take to instill a sense of ethics in the use of computers by their students. M.I.T's Project Athena provides some 800 networked engineering workstations for undergraduates to use in any way they find helpful to their education. Accordingly, Project Athena has assumed that one of its responsibilities is to open a discussion of ethical use with its user community. The primary action that Project Athena has taken is the publication of a set of principles.

These principles are general, for the most part, following M.I.T's usual approach of appealing to basic concepts rather than spelling out many detailed rules. There is no claim that publicizing these principles completely solves any problem nor that it completely answers any question, but it does represent one organization's attempt to take a step in the right direction. Some version of these principles have been posted for about four years, and whenever we have an incident serious enough to ask a student to talk to the director, these principles have provided a useful starting point for the conversation.

Principles of Responsible Use of Project Athena

Project Athena is M.I.T's computing facility for education. It consists of a networked system of workstations and services, and includes communication features that offer many opportunities for members of the M.I.T. community to share information.

With that ability to share comes the responsibility to use the system in accordance with M.I.T's standards of honesty and personal conduct. Those standards, outlined in the M.I.T. Bulletin under academic procedures, call for all members of the community to act in a responsible, ethical and professional way. What follows are guidelines in applying those standards to use of Project Athena facilities.

Intended Use

The hardware granted to Project Athena, and the software licensed for that hardware, are intended for educational use, broadly construed, by members of the M.I.T. community. Use of Athena resources by anyone outside M.I.T. requires approval of the provost, and the sale of such use is improper. The use of Project Athena's facilities for sponsored research activities that normally would make use of other M.I.T. facilities requires specific authorization of the director.

Privacy and Security

The operating systems used by Project Athena encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing. Users must supplement the system's security mechanisms by using the system in a manner that preserves the privacy of others.

For example, users should not attempt to gain access to the files or directories of another user without clear authorization from the other user (typically that authorization is expressed by setting file access permissions to allow public or group reading). Nor should users attempt to intercept any network communications, such as electronic mail or user-to-user dialog. A shared program should not be stored or communicated on the systems. Examples of such personal information are grades or letters of recommendation.

System Integrity

Actions taken by users intentionally to interfere with or to alter the integrity of the system are out of bounds. Such actions include unauthorized use of accounts, impersonation of other individuals in communications, attempts to capture or crack passwords or encryption, and destruction or alteration of data or programs belonging to other users. Equally unacceptable are intentional efforts to restrict or deny access by legitimate users to the system.

Intellectual Property Rights

Some software and data that reside on the system are owned by users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. Users must abide by these restrictions. Such restrictions may include prohibitions against copying programs or data for use on non-Athena systems or for distribution outside M.I.T., against the resale of data or programs or the use of them for noneducational purposes or for financial gain, and against public disclosure of information about programs (e.g., source code) without the owner's authorization. It is the responsibility of the owner of protected software or data to make any such restrictions known to the user. □

Jerome H. Saltzer
Athena Project, M.I.T.

MIT Athena Project

(Student handbook)
1985-1986

CPSR Statement on the Computer Virus

STATEMENT OF ETHICS

The so-called computer virus that swept through a national computer network, the Internet, in early November (1988) is a dramatic example of the vulnerability of complex computer systems. It temporarily denied service to thousands of computer users at academic, business, and military sites. An estimated 6,000 computers across the country were affected in only a few hours. Fortunately, the program was not designed to delete or alter data—the impact of a malicious virus would have been immeasurable.

This was an irresponsible act that cannot be condoned. The Internet should not be treated as a laboratory for uncontrolled experiments in computer security. Networked software is intrinsically risky, and no programmer can guarantee that a self-replicating program will not have unintended consequences.

The value of open networks depends upon the good will and good sense of computer users. Computer professionals should take upon themselves the responsibility to ensure that systems are not misused. Individual accountability is all the more important when people work together through a network of shared resources. Computer professionals should establish and encourage ethics based on the shared needs of network users. We also encourage educators to teach these ethics.

The questions of legal responsibility in this instance are ultimately for our legal system to resolve. The questions confronting computer professionals and others concerned about the future of our technology policy go well beyond this particular case. The incident underscores our society's increasing dependence on complex computer networks. Security flaws in networks, in computer operating systems, and in management practices have been amply demonstrated by break-ins at Stanford University, by the penetration of national research networks, and by the "Christmas virus" that clogged the IBM internal network last December.

Computer Professionals for Social Responsibility (CPSR) believes that this incident should prompt critical review of our dependence on complex computer networks, particularly for military and defense-related functions. The flaws that permitted the recent virus to spread will eventually be fixed, but other flaws will remain. Security loopholes are inevitable in any computer network and are prevalent in those that support general-purpose computing and are widely accessible.

An effective way to correct known security flaws is to publish descriptions of the flaws so that they can be corrected. We therefore view the efforts to conceal technical descriptions of the recent virus as short-sighted.

CPSR believes that innovation, creativity and the open exchange of ideas are the ingredients of scientific advancement and technological achievement. Computer networks, such as the Internet, facilitate this exchange. We cannot afford policies that might restrict the ability of computer researchers to exchange their ideas with one another. More secure networks, such as military and financial networks, sharply restrict access and offer limited functionality. Government, industry, and the university community should support the continued development of network technology that provides open access to many users.

The computer virus has sent a clear warning to the computing community and to society at large. We hope it will provoke a long overdue public discussion about the vulnerabilities of computer networks, and the technological, ethical and legal choices we must address. □

Gary Chapman
Executive Director
Computer Professionals for Social Responsibility

Computer Professionals for Social Responsibility

(Member newsletter)
January, 1989

NSF Poses Code of Networking Ethics

STATEMENT OF ETHICS

The network worm (sometimes called virus) affair raises issues that are very important to our field. Both the BITNET Board of Trustees and the CSNET Executive Committee have been struck by the fact that many public comments on the event have contained statements such as:

"We learned from it."

"We will make sure technically it will not happen again."

"He did us a favor by showing..." unaccompanied by expressions of ethical concern.

As a profession we have succeeded technically in creating facilities—the BITNET, CSNET and other components of the national research network—which are now critical to the conduct of science and engineering in our nation's academic, industrial, and government research laboratories. Further, this technology has spread within our nation's commercial research and development organizations and even into their manufacturing and marketing.

Just as medical malpractice can have a serious effect on an individual's health, one of the costs of our success is that we are now in a position where misuse of our national and private computer networks can have as serious an effect on the nation's economic, defense, and social health. Yet while almost every medical college has at least one course on medical ethics and insists on the observance of ethical guidelines during practice, computer scientists seem to avoid such non-scientific issues.

The worm *experiment* caused a major disruption in the research community. Among other points of attack, the worm exploited a trapdoor that has been distributed as a software *feature*. Many hours of talent were wasted finding and curing the problems raised by this *gene*. Many additional hours were lost when researchers were unable to access supercomputers and mail systems due to system overload and network shutdown.

We condemn the perpetration of such experiments, games, or features by workers in our field, be they students, faculty, researchers or providers. We are especially worried about widespread tendencies to justify, ignore, or perpetuate such breeches. We must behave as do our fellow scientists who have organized around comparable issues to enforce strong ethical practices in the conduct of experiments.

We propose to join with the relevant professional societies and the national research networks to form a Joint Ethics Committee charged with examining existing statements of professional ethics and modifying them as necessary in order to create a strong statement of networking ethics and recommendations for appropriate enforcement procedures.

In its biannual meeting last December the Division Advisory Panel (DAP) of the National Science Foundation (NSF) Division of Networking and Communications Research and Infrastructure (DNCRI) resolved to unanimously support the statement of BITNET/CSNET on the breach of ethics implied by the worm. The group also unanimously endorsed the following statement:

Ethical Network Use Statement

The DAP of the NSF DNCRI deplores lapses of ethical behavior which cause disruption to our national network resources. Industry, government and academe have established *computer* networks in support of research and scholarship. Recent events have accentuated the importance of establishing community standards for the ethical use of networks. In this regard, the DNCRI DAP defines as unethical any activity which purposefully or through negligence:

a. disrupts the intended use of the networks
b. wastes resources (people, bandwidth or computer)
c. destroys the integrity of computer-based information
d. compromises the privacy of users
e. consumes unplanned resources for control and eradication.

We encourage organizations managing and operating networks to adopt and publicize policies and standards for ethical behavior. We also encourage these organizations to adopt administrative procedures to enforce appropriate disciplinary responses to violations and to work with appropriate bodies on drafting legislation in this area. □

David J. Farber
Chair
DNCRI DAP

NSF

(DAP Panel minutes)
November 29-30, 1988

Themes in the Ethics Statements

- Tensions between research and professionalization
- Individual responsibility and the end user
- The relationship between ethics and education
- Computers as (potentially wasted) capital
- Tacit notions of privacy

Themes in the Ethics Statements

- Tensions between research and professionalization
- Individual responsibility and the end user
- The relationship between ethics and education
- Computers as (potentially wasted) capital
- Tacit notions of privacy

Tensions between research and professionalization

"The worm ***experiment*** caused a major disruption in the research community. … Many hours of talent were wasted finding and curing the problems raised by this ***game***."

NSF Ethics Statement, June 1989 *CACM* Issue, p. 688

Tensions between research and professionalization

"The worm ***experiment*** caused a major disruption in the research community. … Many hours of talent were wasted finding and curing the problems raised by this ***game***."

"Yet while almost every medical college has at least one course on medical ethics and insists on the observance of ethical guidelines during practice, **computer scientists seem to avoid such non-scientific issues**."

NSF Ethics Statement, June 1989 *CACM* Issue, p. 688

Tensions between research and professionalization

"The worm ***experiment*** caused a major disruption in the research community. … Many hours of talent were wasted finding and curing the problems raised by this ***game***."

"Yet while almost every **medical college** has at least one course on **medical ethics** and insists on the observance of ethical guidelines **during practice**, **computer scientists seem to avoid such non-scientific issues**."

NSF Ethics Statement, June 1989 *CACM* Issue, p. 688

Ethics as a part of professionalization

> "Just as **medical malpractice** can have a serious effect on an individual's health, **one of the costs of our success** is that we are now in a position **where misuse of our national and private computer networks** can have as serious an effect on the nation's **economic, defense, and social health**."

NSF Ethics Statement, June 1989 *CACM* Issue, p. 688

> "The incident underscores our society's **increasing dependence** on complex computer networks."

CPSR Ethics Statement, June 1989 *CACM* Issue, p. 699

"The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up **technical and procedural mechanisms to make the Internet more resistant to disruption**.

IAB Ethics Statement, June 1989 *CACM* Issue, p. 710

Ethics as a part of professionalization

"Just as **medical malpractice** can have a serious effect on an individual's health, **one of the costs of our success** is that we are now in a position **where misuse of our national and private computer networks** can have as serious an effect on the nation's **economic, defense, and social health**."

NSF Ethics Statement, June 1989 *CACM* Issue, p. 688

"The incident underscores our society's **increasing dependence** on complex computer networks."

CPSR Ethics Statement, June 1989 *CACM* Issue, p. 699

"The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up **technical and procedural mechanisms to make the Internet more resistant to disruption**. Such security, however, **may be extremely expensive and may be counterproductive** if it inhibits the free flow of information which makes the Internet so valuable."

IAB Ethics Statement, June 1989 *CACM* Issue, p. 710

"CPSR believes that **innovation, creativity and the open exchange of ideas** are the ingredients of scientific advancement and technological achievement. Computer networks, such as the Internet, facilitate this exchange. **We cannot afford policies that might restrict** the ability of computer researchers to exchange their ideas with one another."

CPSR Ethics Statement, June 1989 *CACM* Issue, p. 699

What is “ethics” in relation to professionalization?

“Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise **great caution** in the conduct of their work. **Negligence in the conduct of Internet-wide experiments is both irresponsible and unacceptable.**”

IAB Ethics Statement, June 1989 *CACM* Issue, p. 710

What is “ethics” in relation to professionalization?

“Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise **great caution** in the conduct of their work. **Negligence in the conduct of Internet-wide experiments is both irresponsible and unacceptable.**”

“…unethical and unacceptable … activity … purposely:

(a) seeks to gain unauthorized access to the resources of the Internet,

(b) disrupts the intended use of the Internet,

(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information, and/or

(e) compromises the privacy of users.”

Principles of Responsible Use

- Intended Use
- Privacy and Security
- System Integrity
- Intellectual Property Rights

IAB Ethics Statement, June 1989 *CACM* Issue, p. 710

MIT Ethics Statement, June 1989 *CACM* Issue, p. 704

Themes in the Ethics Statements

- Tensions between research and professionalization
- **Individual responsibility and the end user**
- The relationship between ethics and education
- Computers as (potentially wasted) capital
- Tacit notions of privacy

Individual responsibility and the end user

"The value of open networks depends upon the **good will and good sense of computer users**. Computer professionals **should take upon themselves the responsibility** to ensure that systems are not misused. **Individual accountability** is all the more important when people work together through a network of shared resources."

CPSR Ethics Statement, June 1989 *CACM* Issue, p. 699

"In the final analysis, the health and well-being of the **Internet is the responsibility of its users who must, uniformly, guard against abuses** which disrupt the system and threaten its long-term viability."

IAB Ethics Statement, June 1989 *CACM* Issue, p. 710

With that ability to share comes the responsibility to use the system in accordance with M.I.T.'s **standards of honesty and personal conduct**.

MIT Ethics Statement, June 1989 *CACM* Issue, p. 704

Individual responsibility and the end user

"…unethical and unacceptable … activity … purposely:

(a) seeks to gain unauthorized access to the resources of the Internet,

(b) disrupts the intended use of the Internet,

(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information, and/or

(e) compromises the privacy of users."

IAB Ethics Statement, June 1989 *CACM* Issue, p. 710

Principles of Responsible Use

- Intended Use
- Privacy and Security
- System Integrity
- Intellectual Property Rights

MIT Ethics Statement, June 1989 *CACM* Issue, p. 704

Individual responsibility and the end user

"Choosing the **proper boundaries between functions** is perhaps the primary activity of the computer system designer. … The [end-to-end principle] appeals to application requirements and provides a rationale for moving a function upward … **closer to the application that uses the function**."

Salzer, Reed, and Clark, End-To-End Arguments in System Design, 1984, p. 277

(And see Cooper and Vidan, Making the Unaccountable Internet, 2022)

"…unethical and unacceptable … activity … purposely:

(a) seeks to gain unauthorized access to the resources of the Internet,

(b) disrupts the intended use of the Internet,

(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information, and/or

(e) compromises the privacy of users."

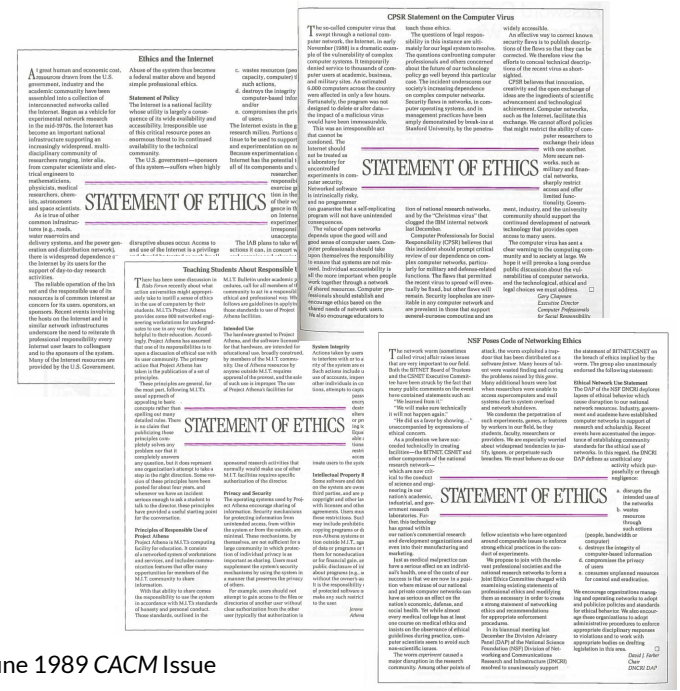
IAB Ethics Statement, June 1989 *CACM* Issue, p. 710

Principles of Responsible Use

- Intended Use
- Privacy and Security
- System Integrity
- Intellectual Property Rights

MIT Ethics Statement, June 1989 *CACM* Issue, p. 704

Resonance with AI ethics today



Ethics and the Internet

STATEMENT OF ETHICS

Teaching Students About Responsible I

STATEMENT OF ETHICS

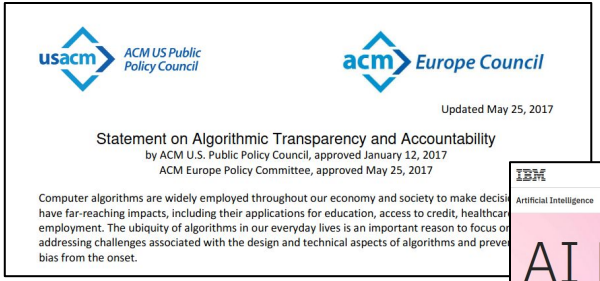
CPSR Statement on the Computer Virus

STATEMENT OF ETHICS

NSF Poses Code of Networking Ethics

STATEMENT OF ETHICS

June 1989 *CACM* Issue



usacm ACM US Public Policy Council

acm Europe Council

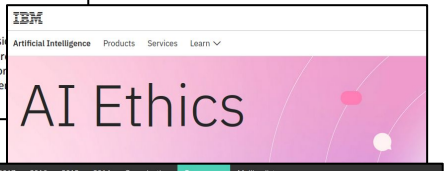
Updated May 25, 2017

Statement on Algorithmic Transparency and Accountability

by ACM U.S. Public Policy Council, approved January 12, 2017

ACM Europe Policy Committee, approved May 25, 2017

Computer algorithms are widely employed throughout our economy and society to make decisi
have far-reaching impacts, including their applications for education, access to credit, healthcar
employment. The ubiquity of algorithms in our everyday lives is an important reason to focus or
addressing challenges associated with the design and technical aspects of algorithms and preve
bias from the onset.



IBM

Artificial Intelligence Products Services Learn

AI Ethics

RESPONSIBILITIES ›

Artificial Intelligence at Google: Our Principles

FAT/ML 2018 2017 2016 2015 2014 Organization Resources Mailing list

Scholarship Events Projects Principles and Best Practices

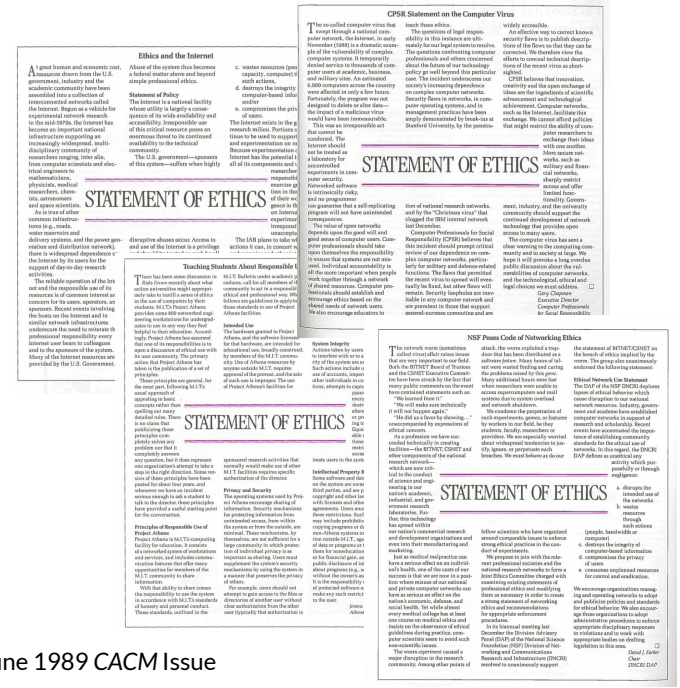
Principles for Accountable Algorithms and a Social Impact Statement for Algorithms

Principles for Accountable Algorithms

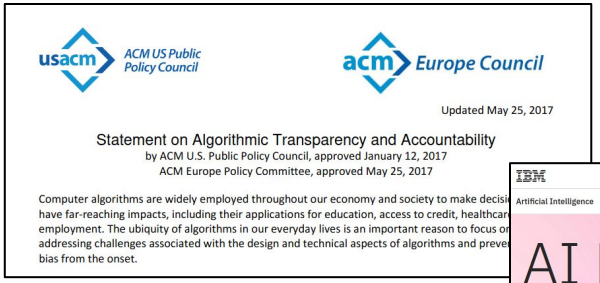
Automated decision making algorithms are now used throughout industry and government, underpinning many processes from dynamic pricing to employment practices to criminal sentencing. Given that such algorithmically informed decisions have the potential for significant societal impact, the goal of this document is to help developers and product managers design and implement algorithmic systems in publicly accountable ways. Accountability in this context includes an obligation to report, explain, or justify algorithmic decision-making as well as mitigate any negative social impacts or potential harms.

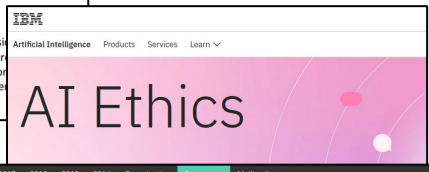
Statements of AI Ethics, Algorithmic Transparency and Accountability, and AI Principles, Today

Resonance with AI ethics today



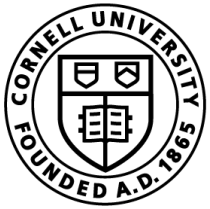
June 1989 *CACM* Issue





Statements of AI Ethics, Algorithmic Transparency and Accountability, and AI Principles, Today

"The American public and its leaders are beginning to be concerned about computing...Clearly, we can no longer ignore public concerns about our profession. We must take control of professional computing or others will control it for us" Bryan Kocher, ACM President, June 1989 *CACM* Issue, p. 660



Cornell Bowers C·IS
College of Computing
and Information Science

"We have met the enemy and it is us":

Debating the ethics of computing in the pages of *CACM*

A. Feder Cooper, Solon Barocas, Karen Levy, and Gili Vidan

Thank you!