

CINDY A. COHN, ESQ.; SBN 145997
McGLASHAN & SARRAIL
Professional Corporation
177 Bovet Road, Sixth Floor
San Mateo, CA 94402
Tel: (415) 341-2585
Fax: (415) 341-1395

LEE TIEN, ESQ.; SBN 148216
1452 Curtis Street
Berkeley, CA 94702
Tel: (510) 525-0817

Attorneys for Plaintiff
Daniel J. Bernstein

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN)
) C 95-00582 MHP
Plaintiff,)
) DECLARATION OF
v.) CARL M. ELLISON
))
UNITED STATES DEPARTMENT OF)
STATE et al.,))
Defendants.)
)
)

I, CARL M. ELLISON, hereby declare:

1. I am currently employed by CyberCash, Inc., at 2100 Reston Parkway, Reston VA 22091, as a cryptography, performance and system architecture expert. I give this declaration in my personal capacity and not on behalf of my employer.
2. I have been a full time professional computer scientist (programmer, system designer and hardware designer) for nearly 30 years, starting in mid 1966, after having been a computer hobbyist since my involvement in a high school computer club in 1959.
3. I was one of the pioneers of computer networking, serving as chief of system programming from 1970 to 1975 at the Utah node of the ARPANET, the predecessor to the Internet. The Utah location for the ARPANET was one of the first locations of what has now evolved as the global Internet.
4. At the University of Utah I was responsible for the design and implementation of an interprocess-communication mechanism which facilitated the development of our network implementation and permitted us to be the first node on the original ARPANet to allow remote login, a basic part of the current functionality of the Internet.
5. For at least the past 5 years, I have used the Internet continuously during work hours and for an average of 1 hour per night at home. I have published my own World Wide Web pages since at least June 1995. I have also been a frequent reader of and contributor to USENET News in various newsgroups.
6. In my nearly 30 years of computer programming I have worked on assemblers, compilers, compiler-compilers, editors, a time sharing nanokernel, signal processing software, data flow software, networking,

network routing, interprocess communication, real time systems, real time 3D graphics algorithms and hardware, data driven hardware in custom VLSI, performance analysis and engineering, fault tolerant system architecture, high speed/low overhead hardware assistance for I/O, cryptographic programming and theoretical analysis. One of the most exciting tasks of my career was my participation in the technical analysis of the 18 1/2 minute gap in one of President Nixon's Watergate tapes.

7. I am fluent in both writing and reading the programming languages known as Assembly Code, FORTRAN, PASCAL, and C. I am competent to read the programming languages known as LISP, PROLOG, ALGOL, PL/I, MAD, and BASIC. I was also instrumental in designing several programming languages, including a dataflow programming language and interpreter known as "function networks", and a language for generating language parsers from source code related to Bacus-Naur Form (BNF).

8. As a person who has been deeply involved in the development and use of computer programming languages, algorithms, and related information, it is my belief that computer languages are used to communicate between human beings and not merely for instructing computers. They are the natural and best means of communication of some kinds of ideas, specifically mathematical concepts in the form of algorithms. Although computer languages are also used as instructions for a computer, it is my contention that a fundamental and essential use for them is for communication between people. I have, for example, written and published computer source code which has almost no use in practice except the instruction of a human reader.

9. Source code could be for communication between two different people or communication between a person at one time and himself at a future time. An early computer science professor of mine taught that the first 10 minutes of a project is pure creation while all remaining work is modification. For that later work, it is important to write code to explain it to the person who will later read it, even when that person might be you. Some large software writing organizations have formal processes called "code audit," in which one person reads the code of another in order to evaluate it for style and correctness.

10. Attached to this declaration are several exhibits which illustrate the basis for my belief.

COMPUTER PROGRAMMING LANGUAGES ARE LANGUAGES

11. My views that computer programming languages are languages in the traditional sense, and that computer programming languages are designed to be read by other humans are based upon my personal experience. They are also echoed in the premier computer programming literature.

12. Among those who agree with my view of computer programming is Professor Donald E. Knuth of Stanford University. Professor Knuth has written perhaps the most well known and well used volumes about computer programming, known as The Art of Computer Programming. In these books, which have been the basic teaching tools utilized by computer programming students for over 20 years, Professor Knuth describes computer programming as a "art," noting that "it can be an aesthetic experience much like composing poetry or music." I Knuth, Art of Computer Programming, preface.

13. In a later volume, called "Literate Programming", Professor Knuth expounds upon this position further. Computer programs are fun to write, and well written computer programs are fun to read. One of life's greatest pleasures can be the composition of a computer program that you know will be a pleasure for other people to read and for yourself to read.

Computer programs can also do useful work. One of life's greatest sources of satisfaction is the knowledge that something you have created is contributing to the progress or welfare of society.

Some people even get paid for writing computer programs!
Programming can therefore be triply rewarding -- on aesthetic, humanitarian, and economic grounds

I have spent a good deal of my life trying to help make computer programming as rewarding as possible, in all three senses. At first I thought programming was primarily analogous to musical

composition -- to the creation of intricate patterns, which are meant to be performed. But lately I have come to realize that a far better analogy is available: **Programming is best regarded as the process of creating works of literature**, which are meant to be read.

Literature of the program genre is performable by machines, but that it not its main purpose. Computer programs that are truly beautiful, useful, and profitable must be readable by people. So we ought to address them to people, not to machines. Knuth, *Literate Programming*, IX (emphasis in original).

14. Professor Knuth's perspective on computer programming is shared by me and by many of my programming colleagues. Writing a computer program is a process of communicating my ideas to other human beings as much as it is a process which may make a machine function. It is unnatural to divorce the two.

COMPUTER PROGRAMMING LANGUAGES IN CACM

15. Computer programming languages have been used to communicate scientific ideas for at least 25 years. Attached hereto as Exhibits A - D are some excerpts from Communications of the Association for Computing Machinery, (CACM). The CACM is the premier publication for the development of computers and computer programming, published since 1957. The Association for Computing Machinery (ACM) has been in existence since 1947. As early as 1967 the CACM included descriptions of ideas expressed in computer code, both alone and in addition to descriptions expressed in English and in mathematical terms.

16. For example, Exhibit A hereto is an article from July, 1967, written by Ira Pohl of Stanford University's Stanford Linear Accelerator Center, which provides as an appendix computer code more precisely illustrating the process, described in the text, i.e. rules for finding a particular kind of path in a graph. The source code assists in illustrating the complex rules to a technical reader.

17. Exhibit B attached hereto is an excerpt from the CACM of July, 1967, in which an entire article is presented as source code. As with all computer code, this code contains comments in English which more fully explain to the reader what the code does but the reader is expected to read the code itself, not merely the comments. All computer languages that I know of have a comment capability -- something which is only necessary if one envisions human readers.

18. Attached hereto as Exhibit C is an excerpt from the August 1967 CACM, giving another example of an article which consists solely of source code.

19. In addition, the Exhibit C includes the August, 1967, statement of the algorithm policy of the Association for Computer Machinery. The policy notes:

It is necessary, but not sufficient for the published algorithm to operate on some machine and give correct answers. It must also communicate a method to the reader in a clear and unambiguous manner. All contributions will be refereed by human beings and by an appropriate compiler.

20. The above paragraph again reflects my own view about both algorithms and computer code, in that they must communicate both to a machine and to a human being in order to be useful, but communication to people is more important than communication to a machine. That is, computer code which does not communicate to human beings is considered unacceptable if produced by a computer professional, while computer code which can be read by humans but for which there is no compiler or appropriate machine is still useful.

21. Exhibit D is a true and correct copy of a segment of the CACM from September, 1969, which provides various examples of the presentation of technical ideas in source code, in text, and in mathematics.

22. These are but four examples. As a long-standing member of the ACM and a person who has subscribed to the CACM since 1969, I can fairly represent that nearly every single issue of the CACM through the 1970s

included computer code descriptions of ideas either on their own, as in Exhibits B and C, or in conjunction with English descriptions of the ideas and mathematical descriptions of the ideas.

23. Now this same publication function is handled by both print publications and electronically by the Internet, through FTP, USENET News and World Wide Web pages. These electronic publications provide a means for communicating with a technical audience and one finds many technical papers published electronically -- papers including both mathematical expressions and source code.

COMPUTER CODE IS A TOOL OF SCIENTIFIC COMMUNICATION

24. The fact that published technical papers contain computer code alongside English and math demonstrates that source code is a tool for scientific communication. As a scientist, I choose the particular method which I believe is most effective and precise in each instance, to express my ideas. The method may be English, math, computer code, or some other language, depending on my needs.

25. As noted above, as an author of mathematical and technical ideas I decide how best to express the information. I believe this is no different than a non-technical writer deciding whether to express his ideas in an essay, in fiction, or in poetry, and deciding whether to write those ideas in English or French or classical Greek. In my usual practice, both among technically-minded friends and among scientific colleagues, I use computer code as a human language.

COMPUTER LANGUAGE EXPRESSIONS AS ART FORMS

26. As computer programming languages have become more widely used, people have developed serious as well as frivolous uses for them, much as they have for languages such as French or German. For example, on the frivolous side there are contests to see who can make the most dense code. These contests are designed to communicate from a human to a human, but only to demonstrate one's prowess in the abilities and use of the language, rather than to communicate efficiently. Indeed, although these programs are required to function, most perform uninteresting operations and certainly would not be acceptable in the development of commercial software because of the difficulty of reading them. These contests make the point that software must be readable by humans in order to be useful by making unreadability something noteworthy.

27. In addition, many programmers have begun to develop programming languages as an art form in other ways. For example, attached hereto as Exhibit E is a page from the July 1, 1995 Economist, which includes a segment of poetry written in computer language known as PERL. The Economist notes: the rules of PERL replace the scansion and rhyming conventions of traditional poetry -- and are played with in similar ways. The expert poet highlights subtle errors in the rules for emphasis: the sort of intertextual allusion beloved of current literary criticism.

COMMUNICATION OF SCIENTIFIC IDEAS ON THE INTERNET INCLUDES COMMUNICATION OF CODE

28. As the Internet has developed, it has become an important vehicle for technical communication between programmers, engineers, and mathematicians. In fact, one of the ARPAnet's original purposes was the sharing of technical papers and software.

29. Internet newsgroups such as sci.crypt supplement and in some cases replace print publications such as the CACM as locations where new ideas are announced, criticized, developed and discussed. This includes and requires the inclusion of computer code descriptions of ideas, just as it does in print publications.

30. Internet publication of ideas is in many ways superior to paper publication, in that both the transfer of ideas and feedback and criticism are more immediate and direct. A recent radio commentator described the Internet as the largest vanity press the world has ever known. One vehicle for the phenomenal growth of the Internet -- the World Wide Web -- was created by the scientists at CERN in Switzerland for the purpose, among others, of communicating scientific papers, including computer code, to fellow scientists as rapidly as possible.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: _____ CARL M. ELLISON