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. ) DR. ANDREW W. APPEL
) )
UNITED STATES DEPARTMENT OF )
STATE et al., ) )
Defendants. )
)
)

I, Dr. Andrew W. Appel, hereby declare:

1. I am currently a professor of computer science at Princeton University. I teach courses in compilers, programming languages, and software engineering. My research is in efficient compilation of functional programming languages, particularly the language "ML."
2. I received the Ph.D. in Computer Science from Carnegie-Mellon University in 1985. I have been at Princeton University since 1986; as Assistant Professor (1986-92), Associate Professor (1992-95), and Professor (since 1995). I am the Editor in Chief of ACM Transactions on Programming Languages and Systems, the major journal in the field of programming languages. My work as the implementor of the "Standard ML of New Jersey" compiler is well known. Standard ML of New Jersey is research software that has been distributed widely, without charge, on the Internet since 1988. It is now in use at over 100 universities and industrial research and development laboratories.
3. Publication of ideas is a fundamental part of the academic world. Publication of ideas is emphasized in academia because it is vital to the scientific method. This, on a basic level, means that if you have an idea, you toss it out into the "marketplace of ideas" and your peers and others evaluate it, test it and discuss it. This is how we determine which ideas are good and which are faulty.
4. For example, I mention two journal papers:
a. "Efficient Computation of LALR(1) look-ahead sets." F. L. DeRemer and T. Pennello, ACM Transactions on Programming Languages and Systems, October 1982.
This article explains a faster computer algorithm for a certain task, whose utility was justified by a (claimed)

relationship between two classes of programming language grammars.
b. "On the (non-)Relationship between SLR(1) and NQLALR(1) Grammars." M. E. Bermudez and K. M. Schimpf, ACM Transactions on Programming Languages and Systems, April 1988. This article published nearly six years later, described itself as follows:
"A popular but "not-quite" correct technique for computing LALR(1) look-ahead sets has been formalized by DeRemer and Pennello and dubbed NQLALR(1). They also claim that
the class of SLR(1) grammars is a subset of the class of NQLALR(1) grammars. We prove here that no such relationship exists between those two classes. We do so with a counterexample that, ironically, appeared in DeRemer and Pennello's own paper."
5. Clearly, DeRemer and Penello's idea was not as good or useful as they thought, since Bernudez and Schimpf were able to demonstrate its flaws. On the other hand, scientific journals are full of good papers that do advance the state of the art. The way they do so is by reaching their readers, and encouraging the readers to review, test and improve on the ideas.
6. For anyone whose ideas include or involve computer code, this publication process as part of the scientific method includes publication of that code. This is not only computer scientists, but mathematicians, scientists, economists and others whose ideas are described or demonstrated with the help of computer code. Descriptions limited to English or mathematics are not sufficient to appropriately describe many things. They are certainly not sufficient to allow someone else to test many ideas without significant, unnecessary work. Such testing is required for both the scientific method and academic advancement.
7. For example, early in my career (1986) I became convinced that a certain kind of programming language, called "functional", would be useful for a wide variety of applications. Up to that point, functional languages were considered useful only in very specialized applications, and systems that used functional languages were invariably extremely slow (these two points are related, since many uses of computers require speed).
8. I focused my research on the speedy implementation of the functional language ML, implemented in my "Standard ML of New Jersey" software system. In 1987 I published a preliminary paper (with a colleague) describing the system. Also in 1987, I began making the software available, for free, to anyone who wanted to use it. Originally this was done by sending magnetic tapes through parcel post.
9. By 1988 we realized that we could make our software available on the Internet to anyone who wanted to "fetch" it. We did so in order to allow others to test and review it. By 1990 there were over 70 academic and industrial institutions using the software, and by 1994 over 100. It would have been very difficult to sustain this wide a distribution using magnetic tapes, since we were not charging money for the software.
10. From 1987 to the present I have published a series of papers describing the scientific ideas and methods underlying the software. Any academic scientist is expected to describe his innovations in a form where fellow scientists and the world at large can learn from them. However, in the "marketplace of ideas" there are many competitors, and the scientist often has a hard time being heard. When I published my papers, I think that people took them seriously because they knew the software worked well.
11. Distributing computer code on the Internet enables not only the evaluation of ideas, but also their incremental improvement. For example, a compiler for the programming language is typically a large software system, often containing hundreds of "modules," where each module represents one or more scientific ideas and days or weeks of implementation effort. My "Standard ML of New Jersey" compiler, for example, has 422 modules and represents tens of man-years of effort.
12. A typical scientific idea or innovation usually involves just a small set of these modules. If a scientist wants to test his new idea, involving one module, he will still have to implement all the other modules just to demonstrate that his idea works. By distributing the software, I make it possible for a scientist to replace just one module with an innovative one, and use the other modules that I provide.
13. There have been several occasions since 1988 where computer scientists at other institutions have fetched the Standard ML of New Jersey software on the Internet, made modifications to it, and published scientific papers describing their improvements. The lack of freely distributed software would constitute a significant "barrier to entry" to scientists wanting to test innovations.
14. Making computer code available on the Internet is an important avenue for academic advancement. My own career would have been hurt significantly if I had not been able to distribute working computer programs.
15. I also put course materials up on the Internet for student access. Several of Princeton's computer science

courses have "Web Pages", at the address http://www.cs.princeton.edu/courses. Attached hereto as Exhibit "A" is a copy of this web page as of March 1, 1996. By "clicking" on the underlined items with a mouse you can visit the particular site for each class. The sites contain course readings, homework assignments and student input, all of which can contain computer code.

16. I often suggest to students that they post their projects on the Internet for peer and professor evaluation. This allows the students to begin competing early in the "marketplace of ideas", at a stage where their ideas might not be "finished" enough for publication in a scientific journal. Journals can be very slow in publishing papers, and the students only have a short time before they'll be on the job market. When they apply for jobs, it is very important that the academic community already knows of their results and has begun to make judgements of them.

17. Cryptography is an area of applied mathematics, just as many areas of computer science are. It is not, as the government implies, merely a "product" or a "thing" to be used for commercial purposes; it is an academic discipline which is dynamic. This science may also produce useful things for people, as with many sciences, but it changes and grows with new research and insights gained from the academic process. The further development of this discipline requires that cryptographers be able to share their ideas, including the sharing of their computer code.

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

Date:_____ _____

ANDREW W. APPEL