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.) DANIEL J. BERNSTEIN
))
UNITED STATES DEPARTMENT OF)
STATE et al.,))
Defendants.)
)
)

I, Daniel J. Bernstein, declare:
1. I am the Plaintiff in the above-entitled action. I currently reside in Chicago, Illinois. The facts stated herein are known to me of my own personal knowledge; if called upon to testify thereon, I could and would competently do so.
2. I am currently Research Assistant Professor in the Department of Mathematics, Statistics, and Computer Science at the University of Illinois at Chicago. Between August 1991 and May 1995 I was a Ph.D. candidate in the Department of Mathematics at the University of California at Berkeley.
3. Nearly ten years ago, one of my computer accounts was invaded by an intruder. I spent many hours attempting to figure out whether the intruder had destroyed files or simply copied the files he was interested in.
4. Since then I have been interested in computer security. I have made some contributions to the field. For example, I recently released a secure replacement for a notoriously insecure mail-transfer program.
5. Several years ago, a network intruder penetrated a cluster of computers at New York University (NYU). I designed and helped set up a program to monitor the intruder's actions. I saw that these attacks could have been prevented by wide use of cryptography. I wondered why cryptographic software was not built into NYU's systems.

Development of Snuffle

6. At some point I heard that the government controlled encryption exports, but that it permitted exports of encryption technology in the form of specialized "one-way hash functions." This struck me as silly. I

developed a simple algorithm, which I called Snuffle, to convert a one-way hash function into an encryption system. I implemented Snuffle as a tiny computer program, snuffle.c.
7. I continued my work on Snuffle up through version 5.0. The Snuffle 5.0 package includes snuffle.c, unsnuffle.c, and a paper describing Snuffle.
8. I subsequently developed SEOC, an outgrowth of Snuffle. I now use SEOC to protect my own computers from attack.
9. I intend to publish Snuffle. I intend to present my computer program, snuffle.c, as well as a mathematical description of the algorithm. I intend to use several forms of publication: journals; books; conferences around the world; and the electronic discussion group sci.crypt, which is transmitted to all interested parties through the Internet. I would also like to discuss Snuffle with any cryptographer who expresses an interest in it.
10. I hope that my publication of Snuffle will help other people protect their computers from attack; communicate my ideas to others who might find them interesting or important contributions to the field; and subject Snuffle to outside review, testing, evaluation, and modification as part of the normal interchange of scientific and technological ideas.
11. I created Snuffle on my own, without assistance from the Government. I did not design, develop, configure, adapt, or modify it for military applications. It has predominant civil applications, such as protection of privacy and prevention of fraud.

One-Way Hash Functions

12. To use Snuffle one must insert a one-way hash function. My computer program, snuffle.c, does not contain cryptographic source code; all the cryptographic technology is contained in the hash function. If the hash function is strong, the system encrypts strongly. If the hash function is weak, the system encrypts weakly.
13. One-way hash functions are used for many purposes. For example, before a computer stores a password, it feeds the password through a one-way hash function. To check a password later, the computer feeds the password through the same one-way hash function and checks it against the stored result. An intruder who steals the stored password file will
not be able to find the original password except by guessing.
14. It seems to me that what I had previously heard is correct: while the export of cryptography is specifically controlled by the State Department, hash functions are excluded under ITAR 121.1(XIII)(b)(1)(vi). The hash function I used in Snuffle 5.0 is freely exported by Xerox without a license.
15. Other people have published systems that, like Snuffle, employ hash functions for encryption---for example, Zheng-Matsumoto-Imai (1990), Luby-Rackoff (1988), and Gutmann (1993). I think Snuffle is better engineered than those systems, and I would like to publicly discuss the technical details.

CJ Process and Attempts to Clarify

16. As noted above, I had heard about cryptographic export controls before I developed Snuffle. However, I was unaware of the nature or extent of those controls.
17. In early June 1992, I contacted ODTC and spoke with Defendant Oncale. I briefly described Snuffle to him and asked whether I would need a license to publish it. Defendant Oncale told me that I should submit all of my ideas for review under the CJ process.
18. On or about 30 June 1992, I submitted a CJ request to determine whether publication of the Snuffle 5.0 package required a license under the ITAR. Attached hereto as Exhibit A is a true and correct copy of my cover letter for that request. (I do not include with this Declaration any of the actual items I submitted: that would make them public, as court records, in violation of the ITAR. The items are already filed separately under seal with this Court as Exhibits to the Complaint.)
19. On or about 21 August 1992, the Government informed me that I was required to apply for a license. A true and correct copy of the Government's response is attached hereto as Exhibit B.
20. This determination shocked me, since I had thought that I would be free to publish my ideas.
21. I subsequently received a copy of ITAR and saw the definition of "public-domain." I thought that the public-domain rules permitted publication of information, despite what I had previously heard from ODTC. On 19 March 1993, I sent a letter to Defendant William B. Robinson asking him to confirm my understanding of the public-domain rules. Attached hereto as Exhibit C is a true and correct copy of my letter

to Defendant Robinson.
22. In the meantime, I had attempted to obtain clarification of ODTC's CJ determination. In March 1993, Mark Koro confirmed that Snuffle was not "exportable."

Telephone Conversation with Defendant Charles Ray

23. On 26 March 1993, I contacted Charles Ray by telephone in an attempt to clarify the issues that I had raised in my 19 March letter. Attached hereto as Exhibit D is a transcription of that conversation. (Transcript page 300011-300019). It has been recently corrected by me and is now true and correct to the best of my knowledge.
24. During that conversation, I attempted to discover when and how the public domain exception applied, but I was unable to do so. At one point in the conversation I asked: "So you're saying that in this hypothetical case, when this individual knowingly tries to put something in the library which is, you know, a munitions list article, he can't do it." Defendant Ray responded:
No, I'm not going to say he can't do it because I mean, you know, we don't have thought police, we don't have any way of being out there. . . but what I'm saying is should a person do that, should that information later come in, fall into the possession of a foreign entity and it was determined that that information should have been subject to the Arms Export Control Act, and that person knew or should have known, then I would, there's a possibility that that individual would be subject to sanctions for a violation of the Arms Act . . . particularly if it was knowingly. (Transcript page 300014)

25. I then asked him to explain how a person would figure out whether he "knew" that a foreign person or entity would obtain the information from a public library. Defendant Ray responded: "Well, think about it. You put it in a library where anybody who'd walk into the library can get it. You know, a rational person knows that. What was the purpose for putting it in the library? So that anyone who walked into the library could get it right, right?" (Transcript page 300014).
26. I concluded from this part of our conversation that Defendants could hold someone liable for placing Snuffle into a public library.
27. Also during that conversation I asked Defendant Ray: "So you're saying the State Department does care if somebody tried to publish information. . . ." Defendant Ray responded:
Oh yeah, I think, yeah, because our job .. . . see, we're not just an export control . . . I mean we're not an export control agency for economic reasons. Basically our job is to control the flow of technology, munitions, items, information, whatever, that could affect world peace, could upset regional balances, a number of things. (Transcript page 300013)

28. I had previously thought that the Government did not control publication. I concluded from this part of my conversation with Defendant Ray that the Government did, in fact, control publication.
29. Next, I asked Defendant Ray how the First Amendment protections fit into this scheme of regulation. He suggested that if a reporter got his hands on some cryptographic information and published it:
I don't think, you know, freedom of the press would not, and if he published it in such a way that he knew that it would get into the hands of foreign entities, then he would be breaking the law. . . .Freedom of the press doesn't give you the right to break the law knowingly and you know, those reporters who do it knowingly usually do it willing to accept the punishment for their beliefs in the First Amendment. But it wouldn't necessarily protect a person from prosecution. (Transcript page 300017)

30. Finally I asked Ray what the public domain exception actually applied to. He said: "Well, the only think I can think of, and are no longer defense articles, is the technical data related to a lot of software that was taken off the munitions list." When I pressed him for something in the public domain which was still on the munitions list, he was unable to think
of any. (Transcript page 300018)
31. I concluded from this part of our conversation that the "public domain" exception includes nothing. It seems to me that ODTC interprets "is published" as "has been published"; nothing can be in the public domain unless it has already been published, and nothing can be legally published unless it is already in the public domain.

Further Attempts to Understand the Regulations

32. On 2 April 1993 I again wrote to Defendant Robinson. I asked in more detail about the public domain exception: did ITAR apply to creation of information? distribution of a book within the United States? placement of that book on the shelves of bookstores within the United States? subsequent export? A true and correct copy is attached hereto as Exhibit E.
33. In early July 1993, Defendant Robinson responded to a few of my questions. A true and correct copy is attached hereto as Exhibit F. In it, he stated:"[T]he fact that you created Snuffle 5.0 as a hobby does not in itself exempt you [sic] being a manufacturer of defense articles." In addition, he confirmed that "[I]t would appear, however, that Snuffle 5.0 is not in the 'public domain' as defined in the ITAR," although he did not state the reason for this decision.

Second Set of CJ Requests

34. On 15 July 1993, I submitted five separate CJ requests. The requests covered a spectrum from traditional formulas to computer software: my mathematical description of Snuffle; a description of how to encrypt data with Snuffle; a description of how to tell a computer to encrypt data with Snuffle; and my two programs, snuffle.c and unsnuffle.c. True and correct copies of my cover letters accompanying these submissions are attached hereto as Exhibit G.
35. My main purpose in submitting separate requests was to see whether the Government would designate my mathematical description per se as a defense article.
36. On 20 September 1993, I again wrote to Defendant Robinson asking him to clarify several issues raised by his letter of early July: for example, did I really have to register as an arms manufacturer under ITAR merely for having written down my ideas about Snuffle? Attached hereto as Exhibit H is a true and correct copy of my letter to Defendant Robinson.
37. On 5 October 1993, the Government designated my five items as "defense articles" and stated that they were "subject to the licensing jurisdiction of the Department of State." Attached hereto as Exhibit I is a true and correct copy of the Government's letter to me.

Appeal and Government's "Clarification"

38. On 22 September 1993, I appealed the first CJ determination. Attached hereto as Exhibit J is a true and correct copy of my appeal letter.
39. I received no response to my appeal.
40. Because of the similar nature of my CJ Requests and the apparent futility of appeal, I did not appeal the second determination.
41. On 29 June 1995, after I had sued, the Government issued a letter to me stating, despite the clear meaning of their previous CJ determinations, that two of my items appeared to be "technical data" and that my mathematical description appeared to be entirely uncontrolled. Attached hereto as Exhibit K is a true and correct copy of the Government's letter to me.
42. On May 3, 1996, in response to the Court's request that the Defendants state their determination as to my items "without equivocation." (Opinion, footnote 12) my counsel sent a letter to Defendants seeking these determinations. Attached hereto as Exhibit L is a true and correct copy of my counsel's letter. To date Defendants have failed to respond.

Chilling Effect of Government's Actions

43. I have written other scientific papers, algorithms, and computer programs in the field of cryptography that I wish to publish and openly discuss.
44. As a direct result of the ITAR Scheme and my experiences with Snuffle, I have not published or openly discussed these other scientific papers, algorithms, and computer programs.
45. Many of my colleagues have stated that the ITAR Scheme has made them similarly apprehensive about publishing and discussing cryptography.
46. I believe that the science of cryptography suffers from my apprehension and the apprehension of my colleagues, since cryptography does not receive as much benefit as it otherwise would from scientific evaluation, testing, criticism, and modification.

Impact of ITAR Scheme on Me

47. As a direct result of the ITAR Scheme, I have been unable to share my ideas with my foreign colleagues.
48. As a direct result of the ITAR Scheme, I have had trouble sharing my ideas with my U.S. colleagues: instead of publishing my ideas generally to a wide audience, I have been forced to distribute them one by one with pre-identified persons. This has drastically limited the number of U.S. citizens who have reviewed Snuffle 5.0.
49. As a direct result of the ITAR Scheme, my professional reputation and career have been injured.
50. For instance, Bruce Schneier, the author of one of the seminal texts on cryptography, asked me if he could include Snuffle 5.0 in his book. Fearful of the ITAR regulations, especially in light of my conversations with Mr. Ray, noted above, I turned down Mr. Schneier's offer.
51. The field of cryptography is rapidly growing and changing. Even if I am allowed to publish Snuffle at this time, I will have been damaged by the long delay.
52. Cryptographic algorithms and implementations are judged in large part by whether they can withstand use and testing by many users. For example, the RSA algorithm has withstood many years of attack; it is now widely respected. As a direct result of the ITAR Scheme, Snuffle has not received heavy testing.

Impact on My Teaching Activities

53. I have been asked by my employer, the University of Illinois at Chicago, to teach a course in the science of cryptography during the Spring 1997 semester.
54. Like most university professors, I do not check the citizenship of my students, nor do I take attendance in my classes.
55. From my experience at the university, I expect that some of my students will be foreign persons as defined in the ITAR Scheme. I do not discriminate against noncitizens in my classroom.
56. I also expect that some students will attend my lectures without registering for the course. Class lists will not be finalized until after the course begins.
57. To give my students the best possible understanding of the subject, I plan to teach my students about past, current and possible future cryptographic developments, including cutting edge ideas and implementations which have not previously been published.
58. I intend to discuss course materials with my peers and colleagues around the world to obtain feedback that may help my students.
59. I intend to give my students cryptographic software and technical data as defined in the ITAR Scheme, to help them understand various cryptographic ideas. In particular, I plan to show them Snuffle 5.0.
60. I plan to put my course materials and homework assignments, including Snuffle 5.0, on the Internet at the University of Illinois World Wide Web site for convenient access by my students.
61. The University's World Wide Web site is not limited to students. Like the University library, it is open to any person. After I put my course materials onto the site, they will be available over the Internet to any person who wishes to see them, as are the handouts from a graduate mathematics course that I taught in the Fall 1995 semester. Attached hereto as Exhibit M is a true and correct copy of the World Wide Web pages with my handouts from my Fall 1995 course.
62. I also anticipate that some of my students will take their course notes, course materials, software, and other course-related items out of the country, and that some will discuss them with foreign persons.
63. Given my understanding of the ITAR and my discussions with Defendants, I will be unable to teach cryptography without an injunction in this case.

I declare under penalty of perjury that the foregoing is true and correct and that this Declaration was signed in Chicago, Illinois.

Date:

Daniel J. Bernstein