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.) LAWRENCE MILLER
))
UNITED STATES DEPARTMENT OF)
STATE et al.,))
Defendants.)
)
)

I, LAWRENCE MILLER, declare as follows:

1. I am a graduate student in electrical engineering and computer science at The George Washington University ("GWU") in Washington, D.C. I have personal knowledge of the facts set forth herein, unless otherwise indicated, and if called as a witness could and would so testify.
2. In fall term 1995, I was enrolled in a graduate computer science course in computer security (Computer Security Systems I - CS229) (hereinafter "CS229") at GWU, taught by Prof. Lance Hoffman. Prof. Hoffman specializes in information security and edited the 1995 book Building in Big Brother: The Cryptography Policy Debate. The CS229 syllabus (for Spring 1996, which was substantially the same as the Fall 1995 CS229) is
attached as Exhibit A to this Declaration and incorporated by reference.
3. I have been a graduate student at GWU since January 1994. During
my studies at GWU I have found that a high proportion of the students in the engineering school are foreign nationals. In my CS229 class, about 70% of the approximately 30 students were foreign nationals. I know this because students in the class introduced themselves to each other on the first day of class, and stated what country they came from. I believe that at least one of the students was from Iran.
4. CS229 addressed computer security, including the use of cryptography in maintaining computer, communications, and data security. As part of the learning experience, students must do a term project on some aspect of computer security. Each project involves the production of a term paper, accompanying transparency masters, and a World Wide Web ("Web") page presentation related to the project.

5. By putting the Project on the Web, anyone with a Web "browser" like Netscape Navigator could use the Project and learn how it works. The Web is a format for displaying and linking information on "pages." Programs that "browse" the Web can display pages containing text, images, sound, animation and moving video. A page can include "links" to other types of information or resources, so that while viewing one page, one can "click" on a link and be connected to the resource itself, wherever it is. Such links allow people to locate and efficiently view related information even if the information is stored on numerous computers all around the world.

6. The draft project deliverables (term paper, transparency masters, and Web pages) are turned in in triplicate two or three weeks before the end of the term, and two of the three copies are immediately given to other class members for peer review and evaluation. The students receive reviews of their projects from their fellow students within a week and then have a week or two to take those comments into account in producing their final projects.

7. On or about October 15, Prof. Hoffman approved my proposal for a term project ("the Project"), entitled "Public Key Distribution and Automated Notarization," which involved the development and implementation of two pieces of software: a cryptographic key management and certification system, and a cryptographic notarization system. The Project does not actually encrypt or decrypt messages. It manages and distributes keys which can be used to encrypt messages. The Project is also capable of checking digital signatures and acting as an electronic "notary public" which automatically dates and signs documents. Both systems work through Web "forms," and use Philip Zimmerman's Pretty Good Privacy ("PGP") public key encryption software to perform key management, cryptographic certification, and digital signature generation and verification functions.

8. PGP is encryption software which is capable of performing encryption and generating digital signatures. Encryption is a technique which allows users to encode a message using a numerical "key" so as to make the message difficult (hopefully impossible) to read if it is intercepted by someone who does not have the key. PGP uses a type of encryption called "Public Key" because encryption is performed using a two-part key pair, one part being public and one being private. By publishing my "public key" it is possible for people to encode messages which only I can decode using my "private key." Providing "public keys" to other people is therefore an important part of "public key" cryptography.

9. I selected PGP for the Project because it is believed to be very strong, contains useful and secure key management features, includes both encryption and digital signature capabilities, is widely used, and was freely available to me over the Internet. I knew at the time I began the project that PGP is available in a book published by MIT Press.

10. An initial version of the Project, including the cryptographic key management and notarization systems, a written term paper, and an Internet-accessible hypertext document explaining in detail how the software developed for this project works, was to have been submitted for peer review on December 7, 1995. In order for one of my classmates to test the Project for peer review, he or she would need to have PGP; without PGP, the Project could not be tested.

11. In addition to providing network access to cryptographic key management and digital notarization services through the Web, the written Project report and related hypertext documents would explain in detail how the Project works, in particular concentrating on "risk analysis": how secure the system is, how it could be "cracked," and how possible countermeasures could be implemented in a production system to protect the system from being "cracked."

12. In order to provide a complete discussion of the Project, the description of the Project on the Web would include program source code for the software which processes data entered in the forms by users of the Project. The source code contains interfaces to PGP. This source code, when combined with PGP itself, and installed on a Web server, constitutes a complete, networkable cryptographic key management system. Due to the electronic nature of the publication medium, the hypertext Project report, including the source code, were to be in a computer-readable, network-accessible format.

13. The Project would not and does not encrypt. While PGP was to be used to provide notarization and cryptographic key management services, direct access to PGP's encryption features was not to be provided. PGP itself was not to be distributed as part of this project, since the students assigned to review the project will be able to download PGP from a
number of sites both inside and outside the United States. Instead, links to these locations were to be provided from the hypertext project description. The initial version of my project as it existed in October 1995 included a hypertext link to MIT's PGP distribution page, and to a
site in Germany which provided access to PGP. This initial version of my project was located on a workstation in my apartment and not on a public access web server.

HOW EXPORT CONTROLS INTERFERED WITH THE PROJECT

14. While I was aware that there were export controls on cryptography when I began the Project, I did not initially believe that my Project might be subject to these export controls, because it did not encrypt. At this time I was not familiar with the details of cryptography export controls. It was not until after my proposal was approved by Prof. Hoffman that I
learned - from a lecture Prof. Hoffman gave - that arms export controls on encryption were more complex than I had originally thought. In class, I asked Prof. Hoffman about how my Project might be affected, and I got the distinct impression that it had not occurred to him that there would be any kind of legal problem. He suggested that I do some research and summarize
my concerns to him.

15. I went to the State Department's Web page on the Internet and read what was there. From another Internet site I downloaded the text of the International Traffic in Arms Regulations ("ITAR") and studied it. I searched for text referring to cryptography and software. I discovered that "key management" software is specifically mentioned in Category XIII(b)(1) of the U.S. Munitions List ("USML"). I then became concerned that my project might be subject to ITAR.

16. On or about October 30, 1995, I sent a letter to Prof. Hoffman ("the Letter") expressing concern that in doing the Project or the CS229, I might violate the Arms Export Control Act ("AECA") and the ITAR. A copy of the Letter is attached as Exhibit B to this Declaration and incorporated by reference.

17. I was concerned that the class requirements - peer review of the Project by other students in the CS229, publishing the Project on the Web, and providing access to cryptographic key management functions - might in the case of my Project constitute "export" of items controlled under Category XIII(b) of the USML in violation of the AECA and ITAR unless a license was obtained.

18. I was unsure as to how I could complete the Project without risking possible criminal prosecution. In order to test the features of the key management system, the students assigned to review the Project needed to use PGP, since the key management system only works for PGP keys. I believed that within the United States, foreign students could not legally
obtain PGP. Therefore it would be impossible for my foreign classmates to review the Project without either my violating ITAR by giving them a copy of PGP, or their violating ITAR by downloading a copy of PGP.

19. I was also concerned that while the source code of my Project could not function as a "key management" system independently of PGP, it might still fall under Category XIII(b)(5) of the U.S. Munitions List as "ancillary equipment" since it constitutes a component of a "key management" system designed specifically to interface with PGP, which I
believed was restricted under Category XIII(b)(1) of the U.S. Munitions List.

20. I also believed that publication of the Project on the Web might constitute the "export" of cryptographic key management services for which a license would be needed. Prof. Hoffman had distributed to us parts of a 1994 report from the Office of Technology Assessment ("Information Security and Privacy in Network Environments") which clearly stated that providing services could be an export. Based on my understanding of ITAR, I believed that even if we were to restrict access of the Web page to U.S. sites only, ITAR would still be violated if foreign persons accessed the key management functions of the Web page, because the Web page might be said to "perform" a key management service for them. It also seemed that even if access were restricted only to members of CS229, this constituted a serious problem, since many of my classmates were foreign nationals.

21. Because part of the Project constituted a cryptographic key management system, I believed that by publishing the source code used as a front end to PGP, I might violate ITAR if the source code could be read

from outside the United States or if the source code were read by foreign nationals within the United States.
22. Finally, I believed that discussion of how my software worked, and how its security could be broken, which would be a substantial portion of the term paper, might be subject to "export" restrictions as "technical data," i.e., information directly related to cryptographic software.
23. I was unwilling to ignore the possible consequences of violating the ITAR, because I believed that the State Department could at any time declare the Project controlled, and if it did turn out to be controlled, I would subject not only myself and Prof. Hoffman, but possibly my institution, my foreign classmates, and any foreign person who accessed the Project, to criminal and civil liability.
24. I suggested that Prof. Hoffman consider waiving certain of the normal CS229 requirements to prevent the Project from being "exported" to any foreign nationals.
25. Prof. Hoffman was unwilling to waive these requirements of Web publication and peer review. He expressed his belief that these requirements were integral to the learning experience, since people working in scientific fields need experience with publication and with reviewing and being reviewed by peers. He expressed concern to me that if he were to
only permit U.S. citizens to review my Project he might be violating university policy by discriminating against foreign students. I was also concerned that if review of my project were to be restricted I would not have access to the same quality of review as those students whose project reviewers were drawn from the general population of the class, and expressed this concern to Prof. Hoffman.
26. On or about Nov. 11, 1995, Prof. Hoffman decided to extend my deadline for submitting the initial version of the Project and to seek clarification as to the legality of the Project per the CS229 requirements.
27. On or about Nov. 16, 1995, Prof. Hoffman and I jointly made a request ("the Request") to the State Department for guidance as to whether the Office of Defense Trade Controls would require a Commodity Jurisdiction determination, export license, or other approval before I placed my draft deliverable on the Web or had it peer reviewed, as described above. A copy of the Request, which also provides further details on the Project, is attached as Exhibit C to this Declaration and incorporated by reference.
28. On or about Dec. 7, 1995 the draft version of my Project was due. Prof. Hoffman and I agreed that without a clarification from the State Department it would be unwise to proceed with the peer review portion of my Project. Instead of turning in a draft of my Project for peer review, I gave Prof. Hoffman a sealed envelope containing my draft Project on floppy disk and a copy of the Letter I had sent to him earlier. I conspicuously marked the envelope on both sides with my attempt at a "legal disclaimer" because I was concerned that some foreign person might get it and that I would be in trouble if that happened.
29. On or about Dec. 15, 1995, Prof. Hoffman received a response ("the Response") to our Request from the State Department signed by Mr. William J. Lowell, Director, Office of Defense Trade Controls. A copy of the Response is attached as Exhibit D to this Declaration and incorporated by reference. It stated, in pertinent part, that:

> With regard to the technical data, the Department of State does not control technical data "concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in [22 C.F.R.] º 120.11" (22 C.F.R. º 120.10).
>
> No license is required for the activities described in your letter so long as no cryptographic software covered under the Category XIII(b) of the U.S. Munitions List is taken or sent outside of the United States.

30. Due to the delay in obtaining the Response, Prof. Hoffman and I discussed my situation and it was decided that I would take an incomplete in the class. It was clear that it would not be possible to for my Project to be reviewed, revised and graded before the end of the semester. We were also unsure how to proceed based on the contents of the Response.
31. The Response left many questions unanswered. First, by saying "with regard to the technical data," the

Response implied that the Project involved technical data, but it did not specify what parts of the Project in fact were "technical data," if any. Was my Project source code "technical data," or what? It did not seem that my Project could be "public domain," since it was not yet published. It might have been "general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities," but the Response did not actually say so.

32. Second, the Response used the phrase "cryptographic software," implying that some part of the Project was cryptographic software and could not be "taken or sent outside of the United States." But it never actually said that the Project, or any part of it, was cryptographic software.

33. Third, I remained unclear as to whether cryptographic software was "technical data." The Response suggested that it was not technical data, but only by backward inference. By then, I knew that disclosing technical data to a foreign person, even within the United States, was an export; the Response seemed to say that only if cryptographic software were to be "taken or sent outside of the United States" would a license be needed. Thus it was possible that cryptographic software was not technical data.

34. I could not be sure, however, because the Response also stated that technical data "concerning general . . . principles . . . or information in the public domain" was not controlled. The Response could be read to say that PGP fell into one of these exemptions, which would seem to indicate that it was technical data. The problem was that while PGP is generally available to the public, my software was definitely not in the public domain, because I hadn't published it.

35. Furthermore, it was not clear to me what would count as cryptographic software being "taken or sent outside of the United States." Did making information available for access or downloading internationally count as its being "taken or sent outside of the United States?" I believed PGP was cryptographic software for ITAR purposes, but PGP would not be distributed as part of this project. Instead, links to locations where PGP could be obtained were to be provided from the hypertext project description. If someone outside the United States linked to the Project's Web page, and used the link to download PGP from a U.S. location, would I have caused PGP to be "sent or taken outside the United States?" Suppose I
only provided links to PGP residing outside the United States? Then a person outside the United States would be obtaining PGP from a site outside the United States - but would also be doing so via the link which we provided in the United States.

36. Because the Response did not identify which parts of the Project were "technical data" and which parts were "cryptographic software," I did not know what parts of the Project were subject to State Department jurisdiction. Consequently, it remained unclear whether placing the Project on a Web page available internationally was an export for which a
license was needed. Prof. Hoffman expressed the same concern, especially because these issues were likely to arise the next time one of his students proposed a project involving cryptographic software.

37. All these issues remained unclear. In the meantime, I still had an incomplete grade.

38. I discussed the situation with Prof. Hoffman and suggested seeking further clarification about several points: (a) That the cryptographic key management system, when separated from PGP, is not a Category XIII(b) munition, and that the source code for such a system, even when in electronically readable form, constitutes "public domain" information; (b)
That the cryptographic key management system, with PGP included, is a Category XIII(b) munition; (c) That hosting the cryptographic key management system on a publicly accessible computer does not constitute the provision of a defense service; (d) That the acquisition and use of PGP within the United States by foreign nationals who are students for the purpose of evaluating my project does not require an export license, so students could be given a copy of PGP on a floppy disk to test the Project.

39. We did not pursue the matter further formally with the State Department. From my discussions with Prof. Hoffman, the main reasons we did not do so were that the University legal office was not interested, and that we would waste time and effort, given the vagueness of the Response and the likelihood that State would not provide further clarification.

40. Another concern we had in deciding how to act after reviewing the Response was that we knew, based on the ITAR (22 C.F.R. º 126.9), that an "advisory opinion" from the State Department was not binding on it and would not legally protect us. We would have been less concerned if the Response had been more specific, since we would have been comfortable that the peer review process would not have violated ITAR. But since the Response was so vague, I felt that it was of no help whatsoever if the government did initiate legal action

against us, and could even be used against us in court.
41. On or about February 5, 1996, Prof. Hoffman informally contacted a State Department employee, John Sonderman, expressing his puzzlement over the meaning of the Response and emphazing that the problem we faced was bound to recur and that academic institutions need clear guidance. Prof. Hoffman sent me a printed copy of his e-mail message to Mr. Sonderman, and a copy of it is attached as Exhibit E to this Declaration and incorporated by reference.
42. I had to take an incomplete grade in the class as a result of the legal uncertainty surrounding the Project. There is no question in my mind that the ITAR had a negative effect on my classwork - the way we finally went about reviewing my project was to have two students who were U.S. citizens review my project. This review took place the semester after I took CS229, in May 1996. Prof. Hoffman required that the reviewers be U.S. citizens because we felt that the Response did not clarify the situation.
43. The students who reviewed my project were not selected from CS 229, which is very technical. They were instead selected from a public policy class which Prof. Hoffman teaches in the spring. One of the students who reviewed my project had never taken CS 229. I believe that I would have gotten better technical comments if reviewers had been selected from my CS 229 class, as the reviewers for the other students in my CS 229 class were.
44. I am currently revising my Project for final submission, at which time I will receive a grade for CS229. My academic transcript will permanently reflect that I received an incomplete, even after a final grade is submitted.
45. My experience with ITAR definitely left me feeling that if I do cryptography projects in the future as part of my classwork (which well may be the case) I could end up with further problems. I am also concerned that if I propose cryptography projects in the future they may be less likely to be approved by my professors due to the problems I encountered with this project, and the time burden it imposed on both my professor and myself.

TECHNICAL DETAILS OF THE PROJECT

45. The systems which comprised my Project would manage public keys needed to encrypt with PGP in two ways.
46. A person could register a key with the key database. Once keys were registered, the system would act like a phone directory of public keys and allow users to find and download the public keys of other users. Once downloaded these public keys can be used to encrypt messages so that the messages can be securely sent to other users (for instance, once I download a public key I can use my own copy of PGP to encode a message, and then send the encoded message to the "owner" of the public key by electronic mail).
47. It allows users, once they have their first key registered in the key database, to submit additional keys to the server, and to "revoke," or mark as compromised, keys which they previously had registered on the server. Someone might want to do this because they are afraid that someone may have discovered their private key, because they want to use a key with more digits (which would be more secure), or because they want to change their key because it has been in use for a long time, and they are worried that someone may have "broken" their key. The system checks to make sure that a person adding a key already has a valid key. This procedure also uses PGP and is designed to make it nearly impossible for someone to insert a "fake" key into the key database.
48. A digital signature is a number which is generated using a "private key," and which can be checked against the corresponding public key. Therefore, the effect of generating a digital signature for a computer file is similar to signing a piece of paper, because only the true private key can generate a signature decodable by the associated public key. This means that the file was sent by the person with that public key.
49. In addition to doing "key management" as described above, the Project provides a "digital notary" service which uses PGP's public-key digital signature features to digitally sign text documents. The system permits text documents to be entered into a Web "form." Upon request, the system will respond with an unforgeable cryptographic "signature" with the date and time the document was "signed" by the server. Similarly, "signed" documents can be verified by the server using a similar Web form, to which the system responds with a message stating whether or not the signature was valid, and if it was valid, when it was generated.
50. A "form" is a type of Web page which allows someone who accesses the Web page over the Internet to enter information and send this information back to the computer on which the Web page is stored (such a

computer is commonly called a "web server"). In the case of my Project, information sent to the "web server" using a "form" caused the "web server" to execute
software I wrote, which in turn executed PGP to perform the aforementioned cryptographic functions, and which returned the results to the person who filled out the "form."
I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct and that this Declaration was executed at Livermore, California, on this __ day of July, 1996.

_____
LAWRENCE MILLER