CINDY A. COHN, ESQ.; SBN 145997
LEE TIEN, ESQ.; SBN 148216
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

ROBERT CORN-REVERE, ESQ.
Hogan & Hartson L.L.P.
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5600

JAMES WHEATON, ESQ.; SBN 115230
FIRST AMENDMENT PROJECT
1736 Franklin, 8th Floor
Oakland, CA 94612
(510) 208-7744

RICHARD R. WINTER, ESQ.
(*pro hac vice* pending)
SARAH E. PACE, ESQ.
(*pro hac vice* pending)
McBride Baker & Coles
500 West Madison St., 40th Floor
Chicago, Illinois 60661
(312) 715-5700

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN, Plaintiff, v. UNITED STATES DEPARTMENT OF COMMERCE, et al. Defendants.	)	C 95-00582 MHP PLAINTIFFÕS SECOND SUPPLEMENTAL COMPLAINT

TABLE OF CONTENTS

Plaintiff, Daniel J. Bernstein, by and through his attorneys, files this Second Supplemental Complaint alleging as follows:

A. INTRODUCTION

1. Through this Second Supplemental Complaint, Plaintiff challenges the Export Administration Regulations (15 C.F.R. 732 et seq.) (ÒEARÓ) which govern, *inter alia*, the Òexport of encryption itemsÓ from the United States.

2. Recent changes to the regulations dramatically reduced the number of situations in which PlaintiffÕs speech is subject to prior restraint. However, the current regulations continue to bar Plaintiff from participating fully in scientific conferences; they continue to demand, without a warrant, copies of PlaintiffÕs private correspondence; and they continue to impose a prior restraint on some of PlaintiffÕs academic, scientific, and professional activities.

3. As a result, the regulations continue to violate the United States Constitution: specifically, the First Amendment guarantees of freedom of speech and freedom of association; the Fourth Amendment guarantee of freedom from unreasonable searches and seizures; and the Fifth Amendment guarantee of due process.

4. Accordingly, Plaintiff seeks declaratory and injunctive relief to redress the deprivation of his Constitutional rights.

B. BACKGROUND

(1) ITAR Declared Unconstitutional Prior Restraint

5. On February 21, 1995, Plaintiff filed his original complaint in this action alleging that the Arms Export Control Act and its implementing regulations, the International Traffic in Arms Regulations (ÒITARÓ), were unconstitutional on their face and as applied to him. A true and correct copy of the original complaint is attached hereto as ÒExhibit AÓ and incorporated by reference as though set forth fully herein.

6. More specifically, Plaintiff alleged that the licensing requirements for the export of cryptographic software covered by Part 121, Category XIII(b) of ITAR, and the export control over related technical data constituted an impermissible infringement on freedom of speech in violation of the First Amendment.

7. As an initial matter, the District Court held that source code is speech. *See, Bernstein v. Department of State et al.*, 922 F. Supp. 1436 (N.D.Cal. 1996)(denying defendantsÕ motion to dismiss).

8. The District Court then examined whether the ITAR licensing schemeÕs procedural safeguards were adequate to prevent the danger of arbitrary or discriminatory licensing decisions. The District Court concluded that because the ITAR licensing scheme failed to provide a time limit on the licensing decision, failed to provide for prompt judicial review, and failed to impose a duty on the government to go to court and defend a license denial, the ITAR licensing scheme Òas applied to Category XIII(B) acts as an unconstitutional prior restraint in violation of the First Amendment.Ó *See, Bernstein v. Department of State et al.*, 945 F. Supp. 1279 (N.D. Cal. 1996).

(2) EAR Declared Unconstitutional Prior Restraint

9. On December 30, 1996, the Commerce Department issued new regulations ("EAR") controlling most "encryption items," and the same items were removed from control under ITAR. *See,* 61 Fed. Reg. 68572 (1996).

10. On April 16, 1997, Plaintiff filed a First Supplemental Complaint challenging the constitutionality of EAR. A true and correct copy of the First Supplemental Complaint is attached hereto as "Exhibit B" and incorporated by reference as though set forth fully herein.

11. More specifically, Plaintiff alleged that licensing requirements for the export of cryptographic software covered by EAR constituted an impermissible infringement on speech in violation of the First Amendment.

12. The District Court determined on August 25, 1997, that the procedural safeguards afforded under EAR were, "like the ITAR, woefully inadequate." As a result, the District Court held that EAR constituted an unconstitutional prior restraint in violation of the First Amendment. *See, Bernstein v. Department of State et al.*, 974 F. Supp. 1288 (N.D. Cal. 1997).

13. The District Court permanently enjoined Defendants from, *inter alia*, enforcing EAR against Plaintiff "or anyone who uses, discusses or publishes or seeks to use, discuss or publish plaintiff's encryption program and related materials;" and from "threatening, detaining, prosecuting, discouraging or otherwise interfering with plaintiff or any other person described . . . above in the exercise of their federal constitutional rights as declared in this order." *See, Bernstein v. Department of State et al.*, 974 F. Supp. 1288, 1311 (N.D. Cal. 1997).

14. The injunction was stayed pending appeal.

15. On appeal, the Court of Appeals for the Ninth Circuit held that EAR constituted a prior restraint on speech in violation of the First Amendment because it operates as a prepublication licensing scheme that applies directly to, and burdens scientific expression, it vests boundless discretion in government officials, and it lacks

adequate procedural safeguards. A true and correct copy of the Ninth Circuit Opinion dated May 6, 1999 is attached hereto as "Exhibit C."

16. The Ninth Circuit subsequently ordered that the case be reheard *en banc*, and withdrew its May 6, 1999 opinion.

(3) Revised EAR Published

17. On September 16, 1999, before the Ninth Circuit had an opportunity to hear the matter *en banc*, Defendants announced plans to make significant changes to EAR.

18. Defendants made these changes on January 14, 2000. Defendants added, *inter alia*, 15 C.F.R./740.13(e). *See*, 65 Fed. Reg. 2492.

19. Plaintiff, through his attorneys, sent a letter on January 16, 2000, to Defendants in response to these changes. In that letter, Plaintiff stated his concern that EAR continued to interfere strongly with his planned scientific activities. Plaintiff asked many detailed questions regarding EAR.

20. Defendants responded to Plaintiff on February 18, 2000, asserting that Plaintiff's concerns were unfounded, and answering a few of Plaintiff's questions.

21. Some of Defendants' statements to Plaintiff contradicted the plain meaning of the regulations at the time.

22. For example, contrary to the regulations' plain meaning at the time, Defendants stated: "Binary code which is compiled from TSU source code and which is itself publicly available and not subject to licensing or royalty fee can also be exported under the provisions of license exception TSU."

23. On October 19, 2000, Defendants modified EAR, adding 15 C.F.R./ 740.13(e)(2), to make the regulations consistent with this statement to Plaintiff. *See*, 65 Fed. Reg. 62600, 62605.

24. Plaintiff continued negotiating with Defendants, in the hope that EAR would be modified in several further ways to stop interfering with his activities. To date, Defendants have not made any of the additional changes to EAR suggested by Plaintiff.

25. Plaintiff asked Defendants in September 2001 why they had not made certain changes. To date, Defendants have not answered Plaintiff's question.

26. This case was remanded to the District Court in light of the January 14, 2000 changes to EAR. The parties subsequently agreed during a status conference that Plaintiff could file this Second Supplemental Complaint.

C. THE CURRENT EAR

(1) "Encryption Software"

27. ECCN 5D002 controls software "designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature . . ." 15 C.F.R. / 774, Supplement 1, 5D002.c.1; 5A002.a.1.

28. ECCN 5D002 also controls software "designed or modified to perform cryptanalytic functions" as well as software "designed or modified to provide . . . certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria . . ." 15 C.F.R. / 774, Supplement 1, 5D002.c.1; 5A002.a.2; 5A002.a.6.

29. Software is "controlled for EI reasons" under 5D002 if it is an "encryption item" formerly controlled by ITAR.

30. "Encryption items" are defined by EAR to include "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR." 15 C.F.R. / 772.1.

31. EAR does not define the phrase "contain encryption features."

32. EAR defines "encryption software" as "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software." 15 C.F.R. / 772.1.

(2) "Technical Assistance"

33. ECCN 5E002 controls "technology" for the "development," "production," or "use" of software controlled by ECCN 5D002. 15 C.F.R./774, Supplement 1, 5E002.

34. EAR defines "technology" as "[s]pecific information necessary for the "development," "production," or "use" of a product. The information takes the form of "technical data" or "technical assistance." 15 C.F.R./772.1

35. "Technical data" may "take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories." 15 C.F.R./772.1.

36. "Technical assistance" may "take forms such as instruction, skills training, working knowledge, consulting services," and "may involve transfer of "technical data." 15 C.F.R./772.1.

(3) Controls On "Encryption Software"

37. EAR generally requires a license for the "export" or "reexport" of "encryption items" classified under ECCNs 5A002, 5D002, and 5E002. 15 C.F.R./742.15(a).

38. Violation of EAR can result in civil penalties of up to $100,000 per violation, criminal fines of up to $50,000 and/or imprisonment for up to 5 years. Criminal penalties for an individual's "willful" violation include fines of up to $250,000 and/or imprisonment for up to ten years. 15 C.F.R./764.3.

39. The "export of technology or software" not subject to "EI" controls includes "any release of technology or software subject to the EAR" in a foreign country or to a foreign national. 15 C.F.R./734.2(b)(2).

40. Technology or software not subject to "EI" controls is "released" for export in one of three ways: (i) through visual inspection by foreign nationals of U.S.-origin equipment and facilities; (ii) through oral exchanges of information in the United

States or abroad; or (iii) through the application to situations abroad of personal knowledge or technical experience acquired in the United states. 15 C.F.R./734.2(b)(3).

41. The "export of encryption software" is generally defined by EAR as: "actual shipment, transfer, or transmission out of the United States; or "transfer of such software in the United States to an embassy or affiliate of a foreign country." 15 C.F.R./734.2(b)(9).

42. The export of encryption software controlled for "EI" reasons includes the "downloading or causing the downloading, of such software to locations (including electronic bulletin boards and Internet file transfer protocol and World Wide Web sites) outside the U.S., and making such software available for transfer outside the United States, over radio, electromagnetic, photo optical, or photoelectric communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards and Internet file transfer protocol and World Wide Web sites, or any cryptographic software subject to controls under this regulation unless the person making software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States." 15 C.F.R./734.2(b)(9).

43. "Reexport" means "an actual shipment or transmission of items subject to EAR from one foreign country to another foreign country; or release of technology or software subject to the EAR to a foreign national outside the United States." 15 C.F.R./734.2(b)(4).

44. "Reexport of technology or software" means any "release of technology or source code subject to the EAR to a foreign national of another country." 15 C.F.R./734.2(b)(5).

(4) Controls On "Technical Assistance"

45. "Technical assistance" is controlled in two overlapping ways: as "technical assistance" per se, and as "technology" under ECCN 5E002.

46. EAR requires a license for the "export" of "technical assistance" relating to software "controlled for EI reasons." Under EAR: "No U.S. person may, without authorization from BXA, provide technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States of encryption commodities and software that, if of United States origin, would be controlled for EI reasons under ECCN 5A002 or 5D002 . . ." 15 C.F.R. § 744.9(a).

47. EAR also requires licenses for the "export" and "re-export" of "technology" controlled under ECCN 5E002. *See,* 15 C.F.R. § 774, Supplement 1. By definition, "technology" controlled under ECCN 5E002 includes "technical assistance." 15 C.F.R. § 742.15(a).

48. The "mere teaching or discussion of information about cryptography, including, for example, in an academic setting or in the work of groups or bodies engaged in standards development, by itself, would not establish the intent described in this section, even where foreign persons are present." 15 C.F.R. § 744.9(a).

49. EAR does not define "mere teaching," "mere discussion," "information about cryptography," "academic setting," or "establish the intent."

(5) Licensing Procedures

50. License applications for encryption items classified under ECCNs 5A002, 5D002 and 5E002 are reviewed on a "case-by-case basis by BXA, in conjunction with other agencies, to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests." 15 C.F.R. § 742.15(b).

51. All license applications for items classified under ECCNs 5A002, 5D002 and 5E002 must be resolved or referred to the President no later than 90 days from the date an application is entered into BXA's electronic license processing system. There is no time limit that applies once an application is referred to the President. 15 C.F.R. § 750.4(a).

52. Although the regulations do provide for an internal administrative appeal procedure, such appeals need only be completed "within a reasonable time," and final administrative decisions are not subject to judicial review. 15 C.F.R. ' 756.2(c)(1), (2); 50 U.S.C. App. ' 2412(a), (e).

(6) Exception For Publicly Available, Non-"EI" Software

53. "Publicly available software" is not "subject to EAR" if it is not "controlled for EI reasons" under ECCN 5D002. 15 C.F.R. ' 734.3(b)(3).

54. "Publicly available technology" is not "subject to EAR." 15 C.F.R. ' 734.3(b)(3).

55. "Publicly available technology and software" means technology and software that are already published or will be published; arise during or result from fundamental research; are educational; or are included in certain patent applications. 15 C.F.R. '' 734.7; 734.8; 734.9; 772.1.

(7) Exception For Printed Encryption Software

56. A "printed book or other printed material setting forth encryption source code" is not "subject to EAR." Note to 15 C.F.R. ' 734.3(b)(3).

(8) New Exception For Publicly Available Encryption Source Code

57. A new license exception was added to EAR on January 14, 2000. *See*, 15 C.F.R. ' 740.13(e).

58. Section 740.13(e) generally allows "publicly available" "encryption source code" to be "exported or reexported without review" provided "you have submitted written notification to BXA of the Internet location (e.g., URL or Internet address) or a copy of the source code by the time of export." 15 C.F.R. ' 740.13(e)(1).

59. "Encryption source code" is defined by EAR as a "precise set of operating instructions to a computer that, when compiled, allows for the execution of an encryption function in a computer." 15 C.F.R. ' 772.1.

60. EAR does not define "encryption function."

61. Section 740.13(e) applies a similar rule to "object code resulting from the compiling of source code which would be considered publicly available." 15 C.F.R. § 740.13(e)(2).

62. "Encryption object code" is defined by EAR as "[c]omputer programs containing an encryption source code that has been compiled into a form of code that can be directly executed by a computer to perform an encryption function." 15 C.F.R. § 772.1.

63. Section 740.13(e) applies only to source code that is "not subject to an express agreement for the payment of a licensing fee or royalty for commercial production or sale of any product developed with the source code." 15 C.F.R. § 740.13(e)(1).

64. Section 740.17(b)(4)(i) is another license exception, with additional restrictions, applicable to source code subject to such agreements.

65. Section 740.13(e)(3) limits 740.13(e)(1) as follows: "You may not knowingly export or reexport source code or products developed with this source code to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria."

66. EAR defines "knowledge" to include "not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence." 15 C.F.R. § 772.1.

67. Section 740.13(e)(4) states that various forms of Internet publication "would not establish 'knowledge' of a prohibited export or reexport."

68. EAR does not define "establish 'knowledge'".

D. OVERVIEW OF PLAINTIFF'S ACTIVITIES

69. Plaintiff is now a tenured Associate Professor in the Department of Mathematics, Statistics and Computer Science at the University of Illinois at Chicago ("UIC"). Plaintiff teaches courses in mathematics and computer science.

70. Until 1999, Plaintiff deliberately limited the amount of time he spent on research in cryptography. Plaintiff instead focused on research in computational number theory.

71. Plaintiff started spending more time on cryptography in 1999. His current research includes various topics in computational number theory, cryptography, and computer security.

72. Plaintiff has received three grants from the National Science Foundation to support his research. Plaintiff has given 25 invited scientific lectures at conferences around the world.

73. Plaintiff, like many other scientists, now uses Internet web pages as the preferred medium for publishing his work. Plaintiff's web pages include hundreds of thousands of lines of text written by Plaintiff.

74. Plaintiff also uses several media other than web pages. For example, Plaintiff publishes many short articles in Internet newsgroups. Plaintiff also publishes some articles in printed journals and books.

75. Publication is only one part of the scientific process. Plaintiff, like other scientists, frequently communicates in private; often to ask questions, often to answer questions, often to explore new ideas whose scientific merit is unclear.

E. ECC AND MAGC

76. On January 22, 2001, Plaintiff was invited to give a lecture at the "ECC 2001" (Elliptic-Curve Cryptography) conference. ECC 2001 was scheduled for mid-September 2001 at the University of Waterloo in Canada.

77. On May 11, 2001, Plaintiff was invited to give a lecture at the "MAGC 2001" (Midwest Arithmetical Geometry in Cryptography) conference. MAGC 2001 was scheduled for the beginning of November 2001 at the University of Illinois at Urbana-Champaign.

78. Plaintiff's research at the time included fast methods to compute a mathematical function, known as the "P-224 DH key exchange function," which was within the scope of both conferences.

79. The P-224 DH key-exchange function has two primary applications: protecting messages against eavesdropping, and protecting messages against forgery. Both applications combine the key-exchange function with other mathematical functions known as pseudorandom number generators.

80. Plaintiff's research into the P-224 DH key-exchange function was divided into two computational methods: a "64-bit method" and a "53-bit method." Plaintiff decided to give a lecture at ECC 2001 on the 64-bit method, and to give a lecture at MAGC 2001 on the 53-bit method.

81. At the end of August 2001, Plaintiff finished software to compute the P-224 DH key-exchange function using the 64-bit method.

82. Plaintiff did not publish the software at the time; he did not consider it complete without the 53-bit method. Plaintiff sent copies of the software privately to a few colleagues in the United States.

83. Following the September 11, 2001 terrorist attacks, ECC 2001 was rescheduled to the end of October, 2001.

84. On September 26, 2001, Plaintiff finished software to compute the P-224 DH key-exchange function using the 53-bit method.

85. Plaintiff made the complete 64-bit and 53-bit software, called "NISTP224," available on his web pages on September 29, 2001.

86. To protect himself from prosecution, Plaintiff notified Defendants shortly before making NISTP224 available.

87. On October 28, 2001, Plaintiff took the train to Canada for ECC 2001. Plaintiff used the travel time to work on his laptop computer. Among other things,

Plaintiff wrote some experimental pseudorandom number generation software, called ÒProSPRAYÓ.

88. Pseudorandom number generators have many applications. They are widely used to protect messages against eavesdropping and forgery. They are also widely used for computations having nothing to do with information security.

89. More than 100 people attended ECC 2001. Many participants were from outside the United States and Canada. For example, Robert Harley, an Irish mathematician working in France, gave a lecture at ECC 2001 on recent breakthroughs in finding certain mathematical objects useful for cryptography, called Òcharacteristic-2 elliptic curves.Ó

90. Fearful of prosecution under EAR, Plaintiff refrained from showing ProSPRAY to foreign scientists at ECC 2001. For example, Plaintiff wanted to show ProSPRAY to Mr. Harley and solicit Mr. Harley=s comments on the suitability of ProSPRAY for the Compaq Alpha computer architecture, but refrained from doing so.

91. Plaintiff was unable to take advantage of 15 C.F.R./740.13(e) during this trip. The University of Waterloo did not allow visitors to connect their laptop computers to the Internet, so Plaintiff had no way to send a copy of ProSPRAY to Defendants.

92. Fearful of prosecution under EAR, Plaintiff also refrained from working collaboratively on cryptographic software with foreign scientists attending ECC 2001. For example, Plaintiff wanted to sit down at his laptop computer with Mr. Harley and experiment with some interesting technical aspects of Mr. Harley=s method of finding elliptic curves suitable for cryptography, but refrained from doing so.

93. Even if Plaintiff had had email access, it would have been impossible, as a practical matter, for him to send a copy of every new line of software to Defendants during a highly interactive discussion with his colleagues.

94. Plaintiff then traveled to Urbana for MAGC 2001. Fearful of prosecution under EAR, Plaintiff again refrained from similar scientific activities.

F. EXAMPLES OF PLAINTIFFÕS SOFTWARE

(1) SPRAY

95. In 1998, Plaintiff wrote pseudorandom number generation software called ÒSPRAY.ÓSPRAY and ProSPRAY are variants of the same design.

96. Plaintiff designed SPRAY to be used for, *inter alia*, protecting messages against eavesdropping.

97. SPRAY is subject to EAR. *See*, 15 C.F.R./774, Supplement 1, 5A002.

98. SPRAY is Òencryption softwareÓas defined in EAR. *See*, 15 C.F.R./772.1.

99. SPRAY is an Òencryption itemÓas defined in EAR. *See*, 15 C.F.R./772.1.

100. SPRAY is Ócontrolled for EI reasons under ECCN 5D002,Óbecause it is an Òencryption itemÓtransferred from the United States Munitions List. *See*, 15 C.F.R./774, Supplement 1.

101. Plaintiff wrote SPRAY in a programming language called Ò80x86 assembly language.Ó

102. Programs in assembly language are assembled, not Ócompiled.Ó

103. SPRAY is not Òencryption source codeÓas defined in EAR, because it is assembled, not Ócompiled.Ó*See*, 15 C.F.R./772.1.

104. SPRAY is also not Òencryption object codeÓas defined in EAR, because it is not Òencryption source code that has been compiled.Ó*See*, 15 C.F.R./772.1.

105. EAR requires a license for the Òexport Óof SPRAY, because SPRAY is Òencryption software controlled for EI reasonsÓas defined in EAR, but not Òencryption source codeÓas defined in EAR. *See*, 15 C.F.R./734.3(b)(3) and 15 C.F.R. 740.17(e)(1).

106. In his letter of January 16, 2000, Plaintiff specifically asked Defendants about programs written in assembly language.

107. To date, Defendants have not changed EAR to allow the "export" of such programs.

(2) MMECRT

108. Plaintiff is currently writing MMECRT, software to compute a mathematical function called "modular exponentiation."

109. Modular exponentiation is a large part of a mathematical function called the "RSA signature function," which is widely used to protect messages against forgery.

110. Modular exponentiation is also a large part of a mathematical function called the "RSA encryption function," which is widely used to protect messages against eavesdropping.

111. Modular exponentiation is also a large part of many mathematical functions used for non-cryptographic applications.

112. The computational techniques used by Plaintiff in MMECRT are also useful for two other mathematical functions widely used to protect messages against forgery, namely "RSA signature verification" and the "Wegman-Carter authentication function."

113. Plaintiff's goal in writing MMECRT is to popularize a fast method of computing the RSA signature function, RSA signature verification, and the Wegman-Carter authentication function.

114. Because Plaintiff did not "specially design" MMECRT for cryptographic applications other than "authentication or digital signature," MMECRT should not be subject to EAR. *See,* 15 C.F.R./774, Supplement 1, 5A002.

115. However, Defendants have asserted control over other software intended to protect messages against forgery but also potentially usable to protect messages against eavesdropping.

(3) RWB100

116. Plaintiff is currently writing RWB100, software to compute certain variants of the RSA signature function and RSA signature verification.

117. Pseudorandom number generation has several mathematical uses inside signature-related functions. For this reason, RWB100 includes ProSPRAY.

118. It is unclear whether EAR requires a license for the "export" of RWB100.

(4) UIDwall

119. Plaintiff is currently writing UIDwall, software designed to provide an extremely strong security barrier between other programs running on the same computer.

120. UIDwall is subject to EAR, because the level of security designed into UIDwall is "certifiable" at "TCSEC Class B3." *See,* 15 C.F.R./774, Supplement 1, 5A002a.6 and 5D002.

121. UIDwall is "encryption software" as defined in EAR, because it provides confidentiality of information. *See,* 15 C.F.R./772.1.

122. UIDwall includes an interface designed to support external cryptographic software, so UIDwall contains an "open cryptographic interface" as defined in EAR. *See,* 15 C.F.R./772.1.

123. An "open cryptographic interface" is an "encryption feature." *See,* 15 C.F.R./740.17(b)(5).

124. UIDwall is an "encryption item" as defined in EAR, because it is subject to EAR, it is "encryption software" as defined in EAR, and it "contains encryption features." *See,* 15 C.F.R./772.1.

125. UIDwall is "controlled for EI reasons under ECCN 5D002," because it is an "encryption item" transferred from the United States Munitions List. *See*, 15 C.F.R./774, Supplement 1, 5D002.

126. A combination of UIDwall with external cryptographic software would be "encryption source code" as defined in EAR, because it would be a set of instructions to carry out an "encryption function." *See*, 15 C.F.R./772.1.

127. However, UIDwall by itself is not "encryption source code" as defined in EAR. *See*, 15 C.F.R./772.1.

128. EAR requires a license for the "export" of UIDwall, because UIDwall is "encryption software controlled for EI reasons" as defined in EAR, but not "encryption source code" as defined in EAR. *See*, 15 C.F.R./734.3(b)(3) and 15 C.F.R. 740.17(e)(1).

129. It is unclear whether EAR requires a license for the "export" of a combination of UIDwall with external cryptographic software.

G. EDUCATION OUTSIDE THE CLASSROOM

130. Typical Internet newsgroups and mailing lists are open to anyone with Internet access. Anyone can ask a question, and anyone can answer it.

131. There have been approximately two hundred thousand articles on the sci.crypt newsgroup, including a wide variety of questions from people around the world writing various types of encryption software.

132. In 1997, Plaintiff wrote an Introduction to Cryptography set of web pages for the students in his cryptography course at UIC, and then expanded it to answer many frequently asked questions on sci.crypt.

133. Pursuant to a stipulation between Plaintiff and the United States Secretary of Commerce, Plaintiff was able to make the first version of his Introduction to Cryptography available to his students, although not to the public.

134. Plaintiff has continued working on his Introduction to Cryptography since 1997, improving the exposition and adding material to answer more questions.

135. Plaintiff would like to publish his Introduction to Cryptography, for the benefit of everyone interested in cryptography, and in particular for the benefit of all people asking these questions on sci.crypt.

136. However, EAR requires a license for helping people outside certain countries to write "encryption source code." *See,* 15 C.F.R. 744.9.

137. EAR therefore requires a license for the export publication of Plaintiff's Introduction to Cryptography.

H. MIRRORING

138. Plaintiff sometimes publishes, through his Internet web server, copies of documents that he has found elsewhere on the web.

139. Other Internet users sometimes publish copies of Plaintiff's documents through their own Internet web servers. Some of Plaintiff's documents have been republished on hundreds of different computers.

140. The practice of making a document available from several computers around the Internet is generally called "mirroring." The extra copies of the document are called "mirrors." Changes to the original document are not always immediately reflected in the mirrors, despite the terminology, but they are usually reflected within a short time.

141. It is common for large companies to set up several mirrors of their own documents. It is common for Internet web pages at smaller web sites to be mirrored by third parties.

142. Mirroring is essential for extremely popular documents, because there are limits to the number of users who can simultaneously download a document from a single computer. Ten mirrors can handle ten times as many users.

143. Even when it is not essential, mirroring provides many benefits to Internet users. For example, users can download a document much more quickly and reliably if there is a nearby mirror.

144. Plaintiff regularly mirrors documents relevant to his courses so that his students can retrieve the documents even when UICÕs Internet connection is overloaded.

145. Plaintiff has included mirrors of several documents in his Introduction to Cryptography. Plaintiff does not know whether Defendants already have copies of these documents.

146. For example, PlaintiffÕs Introduction to Cryptography includes copies of GnuPG, OpenSSL, and Fortify, software published outside the United States to protect various types of Internet communications against eavesdropping and forgery. It also includes a copy of cbw, classic cryptanalytic software published in violation of ITAR many years ago.

147. EAR demands copies of documents before Òexport,Ó even if those documents are mirrors of previously published documents.

148. PlaintiffÕs Introduction to Cryptography also includes a copy of SFS, software published outside the United States to protect disk drives against espionage.

149. SFS includes Òencryption object code,Ó that is not clearly covered by 15 C.F.R./740.13(e)(2). It is not clear whether EAR requires a license before Òexport,Ó of SFS.

I. SCI.CRYPT AND IRAN

150. Articles posted to the sci.crypt newsgroup are automatically sent to, *inter alia,* computers at several universities in Iran.

151. Under EAR, general Internet publication Òwould not establish Òknowledge,Ó of an export to Iran. *See,* 15 C.F.R. 740.13(e)(4).

152. However, Plaintiff already knows that posting an article to sci.crypt includes sending it to Iran.

153. Plaintiff cannot use 15 C.F.R. 740.13(e) to knowingly send "source code" to Iran. *See,* 15 C.F.R./740.13(e)(3).

154. EAR therefore requires a license before Plaintiff can post "encryption source code" to sci.crypt.

155. In his letter of January 16, 2000, Plaintiff asked Defendants for an explanation of the effect of EAR on Plaintiff's postings to sci.crypt when Plaintiff "knows" that some of the readers are residents of Iran.

156. In a letter dated February 18, 2000, Defendants incorrectly characterized Plaintiff's knowledge as "post-export knowledge," and thereby avoided answering Plaintiff's question.

157. On May 23, 2000, in response to another letter from Plaintiff, Defendants addressed the question of "pre-export" knowledge, and made clear that Defendants were interested only in "direct" transfers to Iran. However, to date, Defendants have not modified EAR accordingly, and Plaintiff's contemplated postings are still subject to criminal prosecution.

J. CURRENT CASE AND CONTROVERSY

158. As a direct result of the acts and omissions of Defendants, their agents and employees, acting in their official capacities under color of federal law, Plaintiff and other persons have been and are deprived of their federal constitutional rights to speak, to publish, to assemble, to receive information, and to engage in academic study, inquiry and publication, guaranteed by the First Amendment to the U.S. Constitution.

159. As a direct result of the acts and omissions of Defendants, their agents and employees, acting in their official capacities under color of federal law, Plaintiff and other persons have been and are deprived of their federal constitutional right to be free from unreasonable searches and seizures, guaranteed by the Fourth Amendment to the U.S. Constitution.

160. Plaintiff is suffering violations of his constitutional rights because of the final agency action by the Defendants promulgating, enforcing and interpreting EAR, and is aggrieved by such action.

161. Unless immediately restrained, the Defendants will continue to apply EAR to Plaintiff, will continue to chill his speech with the threat of prosecution, and will thereby cause him irreparable injury.

162. An actual controversy now exists between Plaintiff and Defendants concerning the constitutional validity of EAR on its face and as applied to him. A judicial declaration is necessary and appropriate at this time in order that Plaintiff may ascertain and enforce his rights, and also to prevent injustice and irreparable injury to Plaintiff.

163. Plaintiff, PlaintiffÕs academic and scientific colleagues and peers, and the public are harmed by PlaintiffÕs inability to disseminate his work freely.

164. No injury will be sustained by the public or Defendants by the grant of injunctive relief.

165. Plaintiff has no adequate remedy in the ordinary course of the law.

SUPPLEMENTAL COUNT I
FREEDOM OF SPEECH IMPAIRED

166. Plaintiff realleges and incorporates by reference all of the allegations contained in all of the previous paragraphs as though the same were fully set forth herein.

167. EAR effectively prohibits Plaintiff from collaborating with foreign scientists at conferences, when the collaboration includes new Òencryption source code.Ó

168. EAR compels Plaintiff to ÒspeakÓ to the government, even though ÒspeakingÓ on the subject, and at the time required, chills PlaintiffÕs publications and private communications on the subject of cryptography.

169. EAR impedes the ability of Plaintiff and others to receive information about cryptography.

170. EAR imposes costs upon Plaintiff's communications through the Internet. Plaintiff has spent more than 500 hours trying to figure out which of his materials Defendants are demanding to see. Plaintiff anticipates a continuing cost of at least 50 hours per year for Plaintiff to review his own publications and private messages under Section 740.13(e)(1).

171. The burdens placed by EAR upon any particular document are determined by the content of that document.

172. EAR, and in particular EAR's demand for copies of "encryption source code," does not serve any compelling or even substantial government interest.

173. EAR, and in particular EAR's demand for copies of "encryption source code," is not narrowly tailored to serve any compelling or even substantial government interest.

174. EAR's demand for copies of "encryption source code" does not apply to printed publications, and thus lacks even a rational basis.

175. EAR therefore constitutes an impermissible regulation of speech, both facially and as applied to Plaintiff, in violation of the First Amendment to the U.S. Constitution.

WHEREFORE, Plaintiff prays for judgment against Defendants as hereinafter set forth.

SUPPLEMENTAL COUNT II

FREEDOM OF ASSOCIATION IMPAIRED

176. Plaintiff realleges and incorporates by reference all of the allegations contained in all of the previous paragraphs as though the same were fully set forth herein.

177. EAR compels Plaintiff to "speak" to the government, even though "speaking" on the subject, and at the time required, impedes Plaintiff's scientific collaborations with foreign colleagues. EAR also impedes the ability of Plaintiff and others to receive information about cryptography.

178. EAR therefore impairs the right to freely teach, learn from, associate with, and collaborate with foreign colleagues and students, and as such, both facially and as applied to Plaintiff, constitutes a violation of the First Amendment to the U.S. Constitution.

WHEREFORE, Plaintiff prays for judgment against Defendants as hereinafter set forth.

SUPPLEMENTAL COUNT III
UNREASONABLE SEARCH AND SEIZURE

179. Plaintiff realleges and incorporates by reference all of the allegations contained in all of the previous paragraphs as though the same were fully set forth herein.

180. Plaintiff has a reasonable expectation in the privacy of his scientific communications with foreign colleagues.

181. EAR demands copies of Plaintiff's private correspondence, when that correspondence includes "encryption source code," and as such constitutes an unreasonable search.

182. EAR does not provide any procedural safeguards against this intrusion into Plaintiff's privacy. Specifically, there is no requirement that the government obtain a warrant prior to searching Plaintiff's private scientific communications, or that application for any such warrant be based upon probable cause.

183. EAR therefore violates the right to be free from unreasonable searches and seizures, both facially and as applied to Plaintiff, and constitutes an impermissible regulation in violation of the Fourth Amendment to the U.S. Constitution.

WHEREFORE, Plaintiff prays for judgment against Defendants as hereinafter set forth.

SUPPLEMENTAL COUNT IV

PRIOR RESTRAINT

184. Plaintiff realleges and incorporates by reference all of the allegations contained in all of the previous paragraphs as though the same were fully set forth herein.

185. Both the District Court and the Ninth Circuit found that the regulations at issue in the First Supplemental Complaint operated as an unconstitutional prior restraint on Plaintiff=s scientific expression. The absence of procedural safeguards that, in part, led both courts to this conclusion was unchanged by any subsequent amendments to the EAR regulations.

186. Under the current EAR, Plaintiff still needs a license before he may engage in any of the following activities through the Internet:

a. publishing SPRAY and other similar software;

b. publishing RWB100 and other similar software;

c. publishing UIDwall and other similar software;

d. publishing mirrors of controlled documents already published outside the United States;

e. posting Òencryption source codeÓ to sci.crypt;

f. publishing his Introduction to Cryptography;

g. otherwise publicly helping people in most countries to write cryptographic software;

h. privately helping citizens of most countries to write cryptographic software, inside or outside the United States.

187. Under EAR, Defendants are not required to either issue a license within a specified brief period of time or to go to court to restrain publication. As such, EAR, both facially and as applied to Plaintiff, constitutes an impermissible prior restraint on free speech in violation of the First Amendment to the U.S. Constitution.

188. EAR does not ensure a prompt final judicial decision reviewing any interim and possibly erroneous denial of a license, and does not require that the burden of proof in any such judicial action be on the government. As such, EAR, both facially and as

applied to Plaintiff, constitutes an impermissible prior restraint on free speech in violation of the First Amendment.

189. The EAA precludes judicial review of licensing decisions. As a result, EAR, both facially and as applied to Plaintiff, constitutes an unconstitutional prior restraint of free speech in violation of the First Amendment.

WHEREFORE, Plaintiff prays for judgment against Defendants as hereinafter set forth.

SUPPLEMENTAL COUNT V

VAGUENESS

190. Plaintiff realleges and incorporates by reference all of the allegations contained in all of the previous paragraphs as though the same were fully set forth herein.

191. EAR fails to give adequate notice to a person of ordinary intelligence concerning the speech it proscribes. *See*, e.g., 15 C.F.R./744.9(a) ("establish the intent"; "mere teaching"; "mere discussion"; "academic setting"; "information about cryptography"); 15 C.F.R./734.3(b) ("electronic media"); 15 C.F.R./740.13(e)(1) ("subject to an express agreement"; "product"; "commercial"; "establish knowledge"); 15 C.F.R./772.1 ("technology"; "technical assistance"; "technical data"; "encryption source code"; "encryption features; "perform an encryption function"; "specially design" and related intent; "contains encryption features"); 15 C.F.R./774, Supplement 1, 5A002 ("transferred from the U.S. Munitions List"; "[d]esigned or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature").

192. As a result, EAR is susceptible to arbitrary and discriminatory enforcement, chills First Amendment freedoms, and is unconstitutionally vague.

WHEREFORE, Plaintiff prays for judgment against Defendants as hereinafter set forth.

SUPPLEMENTAL COUNT VI

OVERBREADTH

193. Plaintiff realleges and incorporates by reference all of the allegations contained in all of the previous paragraphs as though the same were fully set forth herein.

194. EAR is not carefully drawn or authoritatively construed to punish only unprotected speech, is susceptible of application to protected expression, and is therefore unconstitutionally overbroad.

WHEREFORE, Plaintiff prays for judgment against Defendants as set forth below:

1. For a Declaration of this Court:
   a. declaring that the statutes, regulations, policies, practices and conduct complained of herein, are invalid on their face, and therefore unconstitutional and void;

   b. declaring that the statutes, regulations, policies, practices and conduct complained of herein are in violation of the First Amendment to the Constitution of the United States and so are null and void as applied to Plaintiffõs desired conduct, namely, Internet publication, sci.crypt posting, teaching, in-person discussions, private e-mail, or any other form of publication, communication, or disclosure of: SPRAY; MMECRT; RWB100; UIDwall; cryptography software generally; security software generally; software generally; instructions generally; answers to questions regarding cryptography; answers to questions regarding software; or any other information.

2. For Preliminary and Permanent Injunctions enjoining the Defendants, as well as those persons or entities acting on Defendantsõ behalf, and all persons acting in concert or participating with them, from

   a. further and future enforcement, operation or execution of the statutes, regulations, policies, practices and conduct complained of herein, through criminal prosecution or in any other way;

   b. threatening, detaining, prosecuting, discouraging, or otherwise interfering with Plaintiff or any other person in the exercise of their federal constitutional rights;

   c. threatening, detaining, prosecuting, discouraging, or otherwise interfering with Plaintiff or any other person for Internet publication, sci.crypt posting, teaching, in-person discussions,

private e-mail, or any other form of publication, communication, or disclosure of: SPRAY; MMECRT; RWB100; UIDwall; cryptography software generally; security software generally; software generally; instructions generally; answers to questions regarding cryptography; answers to questions regarding software; or any other information.

3. Granting expedited docket treatment to bring this case to trial at the earliest possible time;

4. For attorneysÕ fees incurred herein;

5. For costs of suit incurred herein; and

6. For such other and further relief as the Court deems just and proper.

Dated: January 7, 2002 ELECTRONIC FRONTIER FOUNDATION

By: _____
CINDY A. COHN
LEE TIEN
Attorneys for Plaintiff
DANIEL J. BERNSTEIN