

DEC 9 1 10 PM '96  
FILED  
RICHARD E. ...  
U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN,

Plaintiff,

vs.

UNITED STATES DEPARTMENT OF STATE  
et al.,

Defendants.

107  
No. C-95-0582 MHP

MEMORANDUM AND ORDER

DEC 16 1996

FILED IN CIVIL DOCKET

Plaintiff Daniel Bernstein brought this action against the Department of State and the individually named defendants seeking declaratory and injunctive relief from their enforcement of the Arms Export Control Act ("AECA"), 22 U.S.C. § 2778, and the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. §§ 120-30 (1994), on the grounds that they are unconstitutional on their face and as applied to plaintiff.

Now before this court are cross-motions for summary judgment on the question of whether the licensing requirements for the export of cryptographic devices and software covered by Part 121, Category XIII(b) of the ITAR and the export control over related technical data constitute an impermissible infringement.

For the Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 on speech in violation of the First Amendment.

2 Having considered the parties' arguments and submissions,  
3 and for the reason set forth below, the court enters the  
4 following memorandum and order.

5  
6 BACKGROUND<sup>1</sup>

7 At the time this action was filed, plaintiff was a PhD  
8 candidate in mathematics at University of California at  
9 Berkeley working in the field of cryptography, an area of  
10 applied mathematics that seeks to develop confidentiality in  
11 electronic communication. Plaintiff is currently a Research  
12 Assistant Professor in the Department of Mathematics,  
13 Statistics and Computer Science at the University of Illinois  
14 at Chicago.

15  
16 I. Cryptography

17 Encryption basically involves running a readable message  
18 known as "plaintext" through a computer program that translates  
19 the message according to an equation or algorithm into  
20 unreadable "ciphertext." Decryption is the translation back to  
21 plaintext when the message is received by someone with an  
22 appropriate "key." The message is both encrypted and decrypted  
23 by compatible keys.<sup>2</sup> The uses of cryptography are far-ranging  
24 in an electronic age, from protecting personal messages over  
25 the Internet and transactions on bank ATMs to ensuring the  
26 secrecy of military intelligence. In a prepublication copy of

1 a report done by the National Research Council ("NRC") at the  
2 request of the Defense Department on national cryptography  
3 policy, the NRC identified four major uses of cryptography:  
4 ensuring data integrity, authenticating users, facilitating  
5 nonrepudiation (the linking of a specific message with a  
6 specific sender) and maintaining confidentiality. Tien Decl.,  
7 Exh. E, National Research Council, National Academy of  
8 Sciences, Cryptography's Role in Securing the Information  
9 Society C-2 (Prepublication Copy May 30, 1996) (hereinafter  
10 "NRC Report").

11 Once a field dominated almost exclusively by governments  
12 concerned with protecting their own secrets as well as  
13 accessing information held by others, the last twenty years has  
14 seen the popularization of cryptography as industries and  
15 individuals alike have increased their use of electronic media  
16 and have sought to protect their electronic products and  
17 communications. NRC Report at vii. As part of this  
18 transformation, cryptography has also become a dynamic academic  
19 discipline within applied mathematics. Appel Decl. at 5; Blaze  
20 Decl. at 2.

21 As a graduate student, Bernstein developed an encryption  
22 algorithm he calls "Snuffle." He describes Snuffle as a zero-  
23 delay private-key encryption system. Complaint Exh. A.  
24 Bernstein has articulated his mathematical ideas in two ways:  
25 in an academic paper in English entitled "The Snuffle  
26 Encryption System," and in "source code" written in "C", a

1 high-level computer programming language,<sup>3</sup> detailing both the  
2 encryption and decryption, which he calls "Snuffle.c" and  
3 "Unsnuffle.c", respectively. Once source code is converted  
4 into "object code," a binary system consisting of a series of  
5 0s and 1s read by a computer, the computer is capable of  
6 encrypting and decrypting data.<sup>4</sup>

7  
8 II. Statutory and Regulatory Background

9 The Arms Export Control Act authorizes the President to  
10 control the import and export of defense articles and defense  
11 services by designating such items to the United States  
12 Munitions List ("USML"). 22 U.S.C. § 2778(a)(1). Once on the  
13 USML, and unless otherwise exempted, a defense article or  
14 service requires a license before it can be imported or  
15 exported. 22 U.S.C. § 2778(b)(2).

16 The International Traffic in Arms Regulations, 22 C.F.R.  
17 §§ 120-30, were promulgated by the Secretary of State, who was  
18 authorized by executive order to implement the AECA. The ITAR  
19 is administered primarily within the Department of State by the  
20 Director of the Office of Defense Trade Controls ("ODTC"),  
21 Bureau of Politico-Military Affairs. The ITAR allows for a  
22 "commodity jurisdiction procedure" by which the ODTC determines  
23 if an article or service is covered by the USML when doubt  
24 exists about an item. 22 C.F.R. § 120.4(a). Also contained in  
25 the ITAR are the licensing requirements for defense articles,  
26 22 C.F.R. § 123, and technical data, 22 C.F.R. § 125.

1 Categories of items covered by the USML are enumerated at  
2 section 121.1. Category XIII, Auxiliary Military Equipment,  
3 includes "Cryptographic (including key management) systems,  
4 equipment, assemblies, modules, integrated circuits, components  
5 or software with the capability of maintaining secrecy or  
6 confidentiality of information or information systems . . . ."  
7 22 C.F.R. § 121 XIII(b)(1). A number of applications of  
8 cryptography are excluded, such as those used in automated  
9 teller machines and certain mass market software products that  
10 use encryption. Id.

11 A "defense article" is defined by the ITAR as any item or  
12 technical data that has been designated in the USML. 22 C.F.R.  
13 § 120.6. A "defense service" is any assistance rendered to a  
14 foreign person in the United States or abroad in the  
15 development or use of a defense article, 22 C.F.R. §  
16 120.9(a)(1), or the furnishing of technical data to a foreign  
17 person, 22 C.F.R. § 9(a)(2).

18 "Technical data" is perhaps the most confusing category of  
19 items regulated by the ITAR since it is defined separately and  
20 in relation to defense articles, 22 C.F.R. § 120.10, but is  
21 also defined as a defense article when it is covered by the  
22 USML. See 22 C.F.R. § 120.6. It generally covers information  
23 "which is required for the design development, production,  
24 manufacture, assembly, operation, repair, testing, maintenance  
25 or modification of defense articles. 22 C.F.R. § 120.10. It  
26 also encompasses software directly related to defense articles.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

22 C.F.R. § 120.10(a)(4). Software "includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test operation, diagnosis and repair." 22 C.F.R. § 121.8(f). A person who wants to export software that is not designated on the USML can apply for a technical data license. 22 C.F.R. § 121.8(f).

The definition of technical data includes some noteworthy exemptions. Technical data "does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain . . . ." 22 C.F.R. § 120.10(a)(5). The public domain exemption excludes from technical data information which is "published and generally accessible" to the public through newsstands, bookstores, subscriptions, libraries, conferences and trade exhibitions. 22 C.F.R. § 120.11(a)(1)-(6). The public domain also includes information available to the public through fundamental research at accredited institutions of higher learning:

Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls.

22 C.F.R. § 120.11(a)(8). It is apparent from the ITAR, and neither party appears to dispute it, that the public domain

1 exceptions apply only to technical data and not to defense  
2 articles.

3 Finally, "export" is defined as "[s]ending or taking a  
4 defense article out of the United States in any manner", 22  
5 C.F.R. § 120.17(a)(1), and as "[d]isclosing (including oral or  
6 visual disclosure) or transferring technical data to a foreign  
7 person, whether in the United States or abroad". 22 C.F.R. §  
8 120.17(a)(4).

9  
10 III. Plaintiff's Commodity Jurisdiction Determinations

11 On June 30, 1992 Bernstein submitted a commodity  
12 jurisdiction ("CJ") request to the State Department to  
13 determine whether three items were controlled by ITAR. Those  
14 items were Snuffle.c and Unsnuffle.c (together referred to as  
15 Snuffle 5.0), each submitted in C language source files, and  
16 his academic paper describing the Snuffle system. Complaint  
17 Exh. A. On August 20, 1992 the ODTIC informed Bernstein that  
18 after consultation with the Departments of Commerce and Defense  
19 it had determined that the commodity Snuffle 5.0 was a defense  
20 article on the USML under Category XIII of the ITAR and subject  
21 to licensing by the Department of State prior to export. The  
22 ODTIC identified the item as a "stand-alone cryptographic  
23 algorithm which is not incorporated into a finished software  
24 product." Complaint Exh. B. The ODTIC further informed  
25 plaintiff that a commercial software product incorporating  
26 Snuffle 5.0 may not be subject to State Department control and

For the Northern District of California

1 should be submitted as a new commodity jurisdiction request.

2 Plaintiff and ODTC exchanged copious and contentious  
3 correspondence regarding the licensing requirements during the  
4 spring of 1993. Still unsure if his academic paper had been  
5 included in the ODTC CJ determination of August 20, 1992,  
6 Bernstein submitted a second CJ request on July 15, 1993,  
7 asking for a separate determination for each of five items.  
8 Lowell Decl., Exh. 17. According to plaintiff these items were  
9 1) the paper, "The Snuffle Encryption System," 2) Snuffle.c, 3)  
10 Unsnuffle.c, 4) a description in English of how to use Snuffle,  
11 and 5) instructions in English for programming a computer to  
12 use Snuffle.<sup>5</sup> On October 5, 1993 the ODTC notified Bernstein  
13 that all of the referenced items were defense articles under  
14 Category XIII(b)(1). Complaint Exh. E. By letter dated June  
15 29, 1995, after plaintiff had initiated this action, the ODTC  
16 clarified that its CJ determinations pertained only to  
17 Snuffle.c and Unsnuffle.c, which it had determined to be a  
18 defense article on the USML. Lowell Decl., Exh. 21 at 1. The  
19 ODTC further noted that the two items of explanatory  
20 information fell within the definition of technical data but  
21 that the paper, "The Snuffle Encryption System," did "not  
22 appear to meet the definition of technical data." Lowell  
23 Decl., Exh. 21 at 2. The June 29 letter also explains the  
24 public domain exception to technical data without drawing a  
25 conclusion about the applicability of that exception to the  
26 explanatory information.

1 This court noted, in considering defendants' motion to  
2 dismiss, that Bernstein had every reason to believe his paper  
3 was determined to be on the USML until June 29, 1995, and that  
4 defendants should make a prompt and unequivocal determination  
5 as to the status of the paper. Bernstein, 922 F.Supp. at 1434  
6 & n.12. Plaintiff's counsel wrote to defense counsel on May 3,  
7 1996, seeking, among other things, such a determination.  
8 Lowell Decl., Exh. 22. In a response dated July 25, 1996,  
9 William Lowell, Director of the ODTIC, stated that their letter  
10 of June 29, 1995 had made clear that the paper "is neither a  
11 defense article nor technical data under the ITAR and USML.  
12 Therefore, this item is not subject to the ITAR." Lowell  
13 Decl., Exh. 24 at 1. With respect to the two items determined  
14 to be technical data, Lowell clarified that their publication  
15 or teaching would not be regulated, but that a license would be  
16 required if the object or intent of their export was to furnish  
17 assistance to a foreign person in operating cryptographic  
18 software. Id. at 2.

19 Plaintiff seeks to publish and communicate his ideas on  
20 cryptography. Bernstein asserts that he is not free to teach  
21 the Snuffle algorithm, to disclose it at academic conferences,  
22 or to publish it in journals or online discussion groups  
23 without a license.

24 //

25 //



1 DISCUSSION

2 Plaintiff contends that the licensing scheme under the  
3 ITAR imposes an unconstitutional prior restraint on  
4 cryptographic speech, whether that speech is defined as a  
5 defense article or technical data. Plaintiff further maintains  
6 that a number of terms make the ITAR vague and overbroad in  
7 violation of the First Amendment.

8 Defendants argue that the ITAR, insofar as it regulates  
9 cryptographic software, is content neutral and easily survives  
10 intermediate scrutiny under the First Amendment. In addition,  
11 defendants aver that the technical data provisions do not  
12 regulate scientific or academic speech and therefore do not act  
13 as a prior restraint on speech. Finally, defendants contend  
14 that plaintiff's overbreadth claim, vagueness claim and his  
15 claims under the Administrative Procedure Act ("APA") are  
16 without merit.

17 Both parties sizable briefs in support of their motions  
18 for summary judgment are notable for the contrast of their  
19 approaches. Plaintiff, for his part, argues that the  
20 provisions of the ITAR at issue violate numerous conceivable--  
21 and a few inconceivable--First Amendment doctrines.

22 Defendants' arguments, in contrast, while steering closer to  
23 traditional first amendment analysis, are notable for the  
24 conspicuous absence of discussion of the prior restraint  
25 doctrine.

26 Defendants state in their opposition that the real issue

1 in this case is whether export licensing controls on  
2 cryptographic software violate the First Amendment. The court  
3 agrees that this is the central issue before it and therefore  
4 an appropriate place to begin. Moreover, as this court has  
5 already determined that source code is speech, Bernstein, 922  
6 F. Supp. at 1436, and both parties agree that a licensing  
7 scheme controls the "export" of such speech, the court turns  
8 first to prior restraint analysis.

9  
10 I. Prior Restraint

11 A. Analytical Framework

12 As the Supreme Court has stated, in determining the extent  
13 of the constitutional protection afforded by the guarantees of  
14 the First Amendment, "it has been generally, if not  
15 universally, considered that it is the chief purpose of the  
16 guaranty to prevent previous restraints upon publication."  
17 Near v. Minnesota, 283 U.S. 697, 713 (1931). It is for this  
18 reason that the Court has held: "Any prior restraint on  
19 expression comes to this Court with a 'heavy presumption'  
20 against its constitutional validity." Organization for a  
21 Better Austin v. Keefe, 402 U.S. 415, 419 (1971) (citations  
22 omitted).

23 While prior restraints have often come in the form of  
24 judicial injunctions on publication, see e.g., C.B.S. v. Davis,  
25 510 U.S. 1315 (1994); New York Times Co. v. United States, 403  
26 U.S. 713 (1971), they are also recognized in licensing schemes.

1 See e.g., FW/PBS, Inc. v. Dallas, 493 U.S. 215 (1990); Lakewood  
2 v. Plain Dealer Publishing Co., 486 U.S. 750 (1988).

3 Governments may impose valid time, place and manner  
4 restrictions when they are content neutral, narrowly tailored  
5 to serve a substantial governmental interest, and leave open  
6 alternative channels for communication. See e.g., Clark v.  
7 Community for Creative Non-Violence, 468 U.S. 288, 293 (1984).  
8 However, "even if a government may constitutionally impose  
9 content-neutral prohibitions on a particular manner of speech,  
10 it may not condition that speech on obtaining a license or  
11 permit from a government official in that official's boundless  
12 discretion." Lakewood, 486 U.S. at 764.

13 It is axiomatic that the First Amendment is more tolerant  
14 of subsequent criminal punishment of speech than it is of prior  
15 restraints on the same speech.

16 ☆ The thread running through all these cases is that  
17 prior restraints on speech and publication are the most  
18 serious and the least tolerable infringement on First  
19 Amendment rights. A criminal penalty or a judgment in a  
20 defamation case is subject to the whole panoply of  
21 protections afforded by deferring the impact of the  
22 judgment until all avenues of appellate review have been  
23 exhausted. . . .

24 ☆ A prior restraint, by contrast and by definition, has  
25 an immediate and irreversible sanction. If it can be said  
26 that a threat of criminal or civil sanction after  
27 publication "chills" speech, prior restraint "freezes" it  
28 at least for the time.

29 Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).

30 While the Supreme Court has consistently rejected the idea  
31 that a prior restraint can never be employed, id. at 570, it  
32 nonetheless begins with a presumption of invalidity. The

1 danger inherent in prior restraints is largely procedural, in  
2 that they bypass the judicial process and locate in a  
3 government official the delicate responsibility of passing on  
4 the permissibility of speech. See Freedman v. Maryland, 380  
5 U.S. 51, 58 (1965) (holding that "a noncriminal process which  
6 requires the prior submission of a film to a sensor avoids  
7 constitutional infirmity only if it takes place under  
8 procedural safeguards designed to obviate the dangers of a  
9  censorship system".) Freedman sets forth three procedural  
10 safeguards that have been used by the Supreme Court to examine  
11 licensing schemes: 1) any prior restraint to judicial review  
12 can only be imposed for a brief and specified period during  
13 which the status quo prevails; 2) expeditious judicial review  
14 must be available; and 3) the censor must bear the burden of  
15 going to court to suppress speech and once there bears the  
16 burden of proof. FW/PBS, 493 U.S. at 227 (citing Freedman, 380  
17 U.S. at 58-60).

18 When the risks associated with unbridled licensing schemes  
19 are present to a significant degree, "courts must entertain an  
20 immediate facial attack on the law." Lakewood, 486 U.S. at  
21 759.

22  
23 **B. Analysis**

24 Plaintiff argues that the CJ process, the registration and  
25 fee system and the licensing system under the ITAR all act as  
26 prior restraints on his ability to communicate and publish both

1 his source code and its accompanying technical data.

2 Additionally, plaintiff contends that by failing to meet the  
3 procedural requirements of Freedman the ITAR scheme violates  
4 the First Amendment.

5 Defendants analyze cryptographic software on the basis of  
6 whether it is content based or content neutral and conclude  
7 that export controls on source code do not regulate the content  
8 of speech and are therefore not a prior restraint or otherwise  
9 in violation of the First Amendment. Defendants discuss prior  
10 restraint only with respect to technical data and contend that  
11 the prior restraint cases are inapplicable.

12 The court will analyze Category XIII of the USML and  
13 technical data separately under the prior restraint doctrine.

14  
15 1. Category XIII(b) of the USML

16 A couple of preliminary observations are in order. The  
17 first concerns the nature of the speech involved. Plaintiff  
18 cites Hurley v. Irish-American Gay Group of Boston, \_\_\_ U.S.  
19 \_\_\_, 115 S.Ct. 2338 (1995), to assert that the First Amendment  
20 prevents compelled speech and McIntyre v. Ohio Electronics  
21 Comm'n, \_\_\_ U.S. \_\_\_, 115 S.Ct. 1511 (1995), in support of its  
22 protection of anonymous speech. Based on these cases plaintiff  
23 advances the novel proposition that the First Amendment also  
24 includes the right to speak confidentially, and thus,  
25 encryption is deserving of protection because it facilitates  
26 private communication. It is unnecessary, and this court is

1 unwilling, to reach this issue. The court reiterates its  
2 previous conclusion that source code is speech. Bernstein, 922  
3 F. Supp. at 1436. Software relating to encryption is simply a  
4 topic of speech employed by some scientists involved in applied  
5 research. Hence, Snuffle is speech afforded the full  
6 protection of the First Amendment not because it enables  
7 encryption, but because it is itself speech.

8 Second, defendants assume that if the ITAR export controls  
9 do not restrict the content of protected speech they are not a  
10 prior restraint. This misunderstands the prior restraint  
11 analysis. If a licensing scheme does not employ sufficient  
12 procedural safeguards, it must be invalidated not because it is  
13 necessarily content based but because it bestows on a  
14 government official substantial power to discriminate based on  
15 the content of the speech or to burden speech by delaying a  
16 licensing decision. Lakewood, 486 U.S. at 759; see also  
17 FW/PBS, 493 U.S. at 229 (plurality opinion) (finding that under  
18 the ordinance at issue the city did not pass judgment on the  
19 content of the protected speech but had an indefinite amount of  
20 time to issue license).

21 Category XIII(b) of the USML--directed as it is to  
22 cryptographic software where software includes logic flows,  
23 algorithms and source code--covers speech protected by the  
24 First Amendment. Defendants do not dispute that the State  
25 Department requires a license to export items covered by  
26 Category XIII(b).<sup>6</sup> Furthermore, exportation as defined by the

1 ITAR would appear to include publication where publication,  
2 such as posting software on the Internet or distributing it  
3 freely among colleagues, could be said to be tantamount to  
4 sending it out of the United States "in any manner". 22 C.F.R.  
5 § 120.17(a)(1).

6 A facial challenge on the basis of prior restraint will  
7 lie where a law has a "close enough nexus to expression, or to  
8 conduct commonly associated with expression, to pose a real and  
9 substantial threat of identified censorship risks." Lakewood,  
10 486 U.S. at 759. In Lakewood, a newspaper challenged a city  
11 ordinance which required annual permits for newsracks on public  
12 property and gave the mayor authority to grant or deny  
13 applications for those permits. The Court contrasted laws that  
14 are directed at expression, such as the one governing the  
15 circulation of newspapers, with laws of general applicability  
16 not aimed at conduct commonly associated with expression, such  
17 as a law requiring building permits. Id. at 760-61. The  
18 former risks self-censorship on the part of those applying for  
19 permits and censorship on the part of the decisionmaker. The  
20 latter rarely do.

21 While, as defendants assert, the bulk of the ITAR scheme  
22 may well be viewed as a law of general applicability not aimed  
23 at expression but at controlling the spread of defense-related  
24 commodities abroad, the same cannot be said of Category XIII(b)  
25 of the Munitions List. Category XIII(b) is directed very  
26 specifically at applied scientific research and speech on the

1 topic of encryption. That it regulates encryption in the  
2 interest of national security does not alone justify a prior  
3 restraint. In New York Times Co., 403 U.S. at 714, the Supreme  
4 Court invalidated a prior restraint on classified material that  
5 had been enjoined in the interests of national security. While  
6 that case inspired nine separate opinions on the propriety of  
7 enjoining publication of the Pentagon Papers in The New York  
8 Times and The Washington Post, a majority of Justices found  
9 national security, without more, too amorphous a rationale to  
10 abrogate the protections of the First Amendment. See id. at  
11 719 (Black, J. and Douglas, J., concurring). Justice Brennan  
12 concluded that the First Amendment's ban on prior restraints  
13 could only be overridden in time of war, id. at 726 (Brennan,  
14 J. concurring) (citing Schenck v. United States, 249 U.S. 47  
15 (1919)), and even then, according to Justice Stewart, only when  
16 disclosure would "surely result in direct, immediate, and  
17 irreparable damage to our Nation or its people." Id. at 730  
18 (Stewart, J. and White, J. concurring). Under such an exacting  
19 standard, defendants' interests here, in being able to break  
20 foreign encryption and conduct adequate surveillance in  
21 "furtherance of world peace and the security and foreign policy  
22 of the United States," 22 U.S.C. § 2778(a)(1), are clearly  
23 insufficient without more.

24 However, even though in form Category XIII(b) aims at  
25 speech, it is arguable--and defendants assert--that its purpose  
26 is content neutral. Yet the very nature of the technology



For the Northern District of California

1 blurs the distinction between these two ways of understanding  
2 the constitutionality of a regulation. With respect to  
3 encryption, the stronger the cryptographic algorithm, the  
4 better the science and the more noteworthy the academic speech,  
5 but also the more powerful are its effects and therefore the  
6 greater the interest in government regulation.<sup>7</sup>

7 However, even if the court were to determine that the  
8 regulatory purpose behind Category XIII(b) was content neutral  
9 that would not resolve the issue. The plurality opinion in  
10 FW/PBS suggests that even an otherwise valid licensing scheme  
11 must still contain adequate procedural safeguards in order to  
12 be constitutional. There Justice O'Connor, joined by Justices  
13 Stevens and Kennedy, stated:

14 Because we conclude that the city's licensing scheme lacks  
15 adequate procedural safeguards, we do not reach the issue  
16 decided by the Court of Appeals whether the ordinance is  
17 properly viewed as a content-neutral time, place, and  
18 manner restriction aimed at secondary effects arising out  
19 of the sexually oriented businesses.

20 FW/PBS, 493 U.S. at 223. Thus, the court turns to the  
21 procedural safeguards afforded by the ITAR.

22 As noted above, the Court in FW/PBS read Freedman to hold  
23 that for a licensing scheme to be constitutional, 1) the  
24 licensor must make the licensing decision within a specific and  
25 reasonable period of time; 2) there must be prompt judicial  
26 review; and 3) the censor must bear the burden of going to  
27 court to uphold a licensing denial and once there bears the  
28 burden of justifying the denial. FW/PBS, 493 U.S. at 227-28  
(citing Freedman, 380 U.S. at 58-60).



1        The ITAR scheme, a paradigm of standardless discretion,  
2        fails on every count. This court finds nothing in the ITAR  
3        that places even minimal limits on the discretion of the  
4        licensor and hence nothing to alleviate the danger of arbitrary  
5        or discriminatory licensing decisions. Part 123 governing  
6        licenses for the export of defense articles, 22 C.F.R. § 123,  
7        lays out an extensive list of requirements for those seeking a  
8        license but places no constraints on the ODTC in approving or  
9        denying a license. First, there is no limit to the time in  
10       which the ODTC must make a licensing decision. Second, not  
11       only does the ITAR not provide for judicial review of licensing  
12       decisions, prompt or otherwise, the AECA makes the initial  
13       designation of items as defense articles unreviewable. 22  
14       U.S.C. § 2778(h). Finally, given there is no recourse for  
15       someone denied a license, there is no burden on the ODTC to go  
16       to court to justify the denial. Moreover, applications for  
17       licenses can be disapproved and approved licenses can be  
18       revoked, suspended or amended without prior notice in the  
19       interests of national security or whenever it "is otherwise  
20       advisable". 22 C.F.R. § 126.7(a)(1). While the court is  
21       mindful of the problems inherent in judicial review of ODTC  
22       licensing decisions regarding cryptographic software, both with  
23       respect to the sophistication of the technology and the  
24       potentially classified nature of the licensing considerations,  
25       there must still be some review available if the export  
26       controls on cryptographic software are to survive the

United States District Court  
of California  
in the District of

1 presumption against prior restraints on speech.

2 According to the NRC Report, some of the problems that  
3 standardless discretion invite have been realized among  
4 commercial vendors of cryptographic products.<sup>8</sup> The Report  
5 notes, for example, that virtually all industry representatives  
6 testified that product development was inhibited and trust  
7 eroded by the unpredictability of USML licensing, a lengthy  
8 licensing process and the lack of an independent adjudicating  
9 forum in which to appeal negative licensing decisions. NRC  
10 Report at 4-14, 4-15, 4-17. In addition, the risk of  
11 discriminatory treatment associated with standardless licensing  
12 schemes was reflected in the Report's comments that companies  
13 were reluctant to express their full dissatisfaction with the  
14 rules and implementation of export controls over cryptographic  
15 products for fear that "any explicit connection between  
16 critical comments and their company might result in unfavorable  
17 treatment of a future application for an export license for one  
18 of their products." Id. at 4-29.



19 In FW/PBS, the Court declared that the first two  
20 safeguards required by Freedman--a time limit on the licensing  
21 decision and judicial review--were essential. FW/PBS, 493 U.S.  
22 at 228. The third requirement that the censor bear the burdens  
23 of going to court and justifying its decision, it concluded,  
24 depended on the nature of the licensing scheme. Unlike the  
25 film censorship at issue in Freedman, the ordinance considered  
26 in FW/PBS did not entail "passing judgment on the content of

1 any protected speech" and because the applicants were applying  
2 for a license of their entire business and not just a single  
3 film, the applicant had "every incentive . . . to pursue a  
4 license denial through court." Id. at 607. For these reasons  
5 the plurality opinion concluded that the city was not required  
6 under the First Amendment to bear the burden of going to court  
7 or to bear the burden of proof once there. Id.

8 The ITAR licensing scheme for items listed in Category  
9 XIII(b) of the USML is more like the scheme in Freedman than  
10 FW/PBS. Here the relevant provision of the ITAR is directed at  
11 speech on a particular subject matter--cryptography. The  
12 Supreme Court has held that "the First Amendment's hostility to  
13 content-based regulation extends not only to a restriction on a  
14 particular viewpoint, but also to a prohibition of public  
15 discussion of an entire topic." Burson v. Freeman, 504 U.S.  
16 191, 197 (1992) (citing Consolidated Edison Co. of N.Y. v.  
17 Public Service Comm'n of N.Y., 447 U.S. 530, 537 (1980)).  
18 Furthermore, applicants must apply for a license for each item  
19 covered by Category XIII(b) and like the film distributor  
20 seeking approval of one film, may be deterred from challenging  
21 the licensing decision.

22 For these reasons, this court concludes that the ITAR  
23 licensing scheme of cryptographic software is subject to all  
24 three procedural safeguards. Because it fails to provide for a  
25 time limit on the licensing decision, for prompt judicial  
26 review and for a duty on the part of the ODTC to go to court

1 and defend a denial of a license, the ITAR licensing system as  
2 applied to Category XIII(B) acts as an unconstitutional prior  
3 restraint in violation of the First Amendment.

4  
5 2. The Technical Data Provision

6 The same question addressed above with respect to Category  
7 XIII(b) applies to the technical data provision: whether it  
8 establishes an impermissible system of prior restraints.

9 Plaintiff argues that it does for the same reasons he  
10 advances with respect to Category XIII(b). Plaintiff contends  
11 that despite the exceptions for fundamental research and work  
12 in the public domain, the technical data provisions still sweep  
13 in a good deal of scientific speech and that a law must be  
14 scrutinized based on what it includes rather than what it  
15 excludes. Additionally, plaintiff asserts that the Ninth  
16 Circuit's interpretation of technical data in United States v.  
17 Edler, 579 F.2d 516 (9th Cir. 1978), no longer saves it on  
18 prior restraint grounds because since Edler the AECA was  
19 amended to preclude judicial review.

20 Defendants contend that Edler upheld a technical data  
21 provision that was considerably less friendly to First  
22 Amendment interests and that since then exemptions for academic  
23 research and discussion have been added and clarified. In  
24 addition to the exemptions of general scientific principles and  
25 fundamental research from the definition of technical data,  
26 defendants point to a number of scholarly articles on

1 cryptographic theory that have been published free of ITAR  
2 licensing. Finally, the ODTIC has indicated that it interprets  
3 the technical data provision in a manner consistent with Edler.  
4 49 Fed. Reg. 47683 (Dec. 6, 1984).

5 In Edler the Ninth Circuit reviewed a conviction under the  
6 predecessor of the AECA for unlicensed exportation of technical  
7 data relating to a defense article on the USML. The technical  
8 data at issue in Edler related to a technique of tape wrapping  
9 with applications for missile components. In an appeal of his  
10 conviction, defendant challenged the statute and regulations on  
11 First Amendment grounds. After finding that "an expansive  
12 interpretation of technical data relating to items on the  
13 Munitions List could seriously impede scientific research and  
14 publishing and international scientific exchange," 579 F.2d at  
15 519, the court went on to adopt a narrowing construction to  
16 save the statute. The court construed the statute and  
17 regulations to prohibit only the export of technical data  
18 "significantly and directly related to specific articles on the  
19 Munitions List." Id. at 521. In addition, when information  
20 could have both peaceful and military applications, the court  
21 added a scienter requirement that a defendant "must know or  
22 have reason to know that its information is intended for the  
23 prohibited use." Id. The Ninth Circuit concluded that as  
24 construed the statute and regulations were not overbroad and  
25 not a prior restraint on speech. Id.

26 This court has serious concerns about the viability of the

1 Edler holding, particularly in light of advanced technologies  
2 such as cryptography and other applied sciences.<sup>9</sup> First, the  
3 Ninth Circuit's reasoning in Edler is not only twenty years  
4 old, but more importantly, it was made without the benefit of  
5 the Supreme Court's subsequent interpretation of Freedman and  
6 the procedural safeguards required of regulatory schemes that  
7 license speech. Second, the court notes with some concern that  
8 in practice the technical data provision appears to have been  
9 as confusing to those charged with implementing it as to those  
10 potentially regulated by it. The NRC Report notes that the  
11 rules governing technical data are particularly difficult to  
12 understand, pointing to the fact that a cryptographic algorithm  
13 that is not machine-readable is technical data while the same  
14 algorithm in machine-readable form is a product.<sup>10</sup> The Report  
15 also provides excerpts from the only document it found in which  
16 the ODTC explains how the regulation of technical data relates  
17 to cryptography. NRC Report at 4-47. That 1980 document  
18 appears to be inconsistent with the Edler construction and  
19 suggests that the technical data provision could be used to  
20 directly regulate, and chill, academic discourse. It states:  
21 "The public is reminded that professional and academic  
22 presentations and informal discussions, as well as  
23 demonstrations of equipment, constituting disclosure of  
24 cryptographic technical data to foreign nationals are  
25 prohibited without the prior approval of this office." Id.<sup>11</sup>  
26 Lastly, defendants received between 1978 and 1984 three

Dept. of Justice  
Concussion  
↓

UNENFORCEABLE  
↓

1 separate and extensive memoranda from the Department of  
2 Justice's Office of Legal Counsel, two regarding proposed  
3 revisions to the ITAR and one specifically addressing the  
4 constitutionality of the ITAR restrictions on public  
5 cryptography. Tien Decl., Exhs. A-C. Each of them concludes,  
6 despite further revision and amendment to the ITAR, that the  
7 technical data provisions as they relate to academic and  
8 scientific speech are in violation of the First Amendment.<sup>12</sup>

9 While this court is inclined to agree, despite revisions  
10 to the ITAR since 1984 and especially in light of Freedman and  
11 FW/PBS, Edler remains the law of this Circuit and this court is  
12 bound by its holding.<sup>13</sup> Moreover, Edler was reaffirmed,  
13 albeit in cursory fashion, by the Ninth Circuit in 1989.  
14 United States v. Posey, 864 F.2d 1487, 1496 (9th Cir. 1989).  
15 If the Ninth Circuit wants to reconsider those opinions it is  
16 free to do so, but that decision is theirs to make.

17 However, as this court has found that Category XIII(b) is  
18 unconstitutional, a question the Ninth Circuit has not had an  
19 opportunity to address, the technical data provision--only  
20 insofar as it relates to items in Category XIII(b)--is  
21 unenforceable.

22  
23 II. Vagueness and Overbreadth

24 The doctrines of vagueness and overbreadth have  
25 traditionally been viewed as related and similar doctrines by  
26 the Supreme Court. Kolender v. Lawson, 461 U.S. 352, 358 n. 8

1 (1983) (citations omitted). Vague or overbroad laws deter the  
2 constitutionally protected activity not only of the litigant,  
3 but of third parties not before the court, and for that reason  
4 can be challenged facially. Grayned v. City of Rockford, 408  
5 U.S. 104, 114 (1972). The court will consider each doctrine  
6 briefly with respect to those parts of the statute not already  
7 adjudicated. The court will not address Category XIII(b) but  
8 will consider other provisions and amendments to the technical  
9 data provision that were not in effect at the time of Edler.

10  
11 A. Vaqueness

12 Due process requires that laws clearly define their  
13 prohibitions. Grayned, 408 U.S. at 108. Vague laws are  
14 objectionable for multiple reasons. First, because they do not  
15 "give the person of ordinary intelligence a reasonable  
16 opportunity to know what is prohibited," they do not provide  
17 fair warning to those who wish to act lawfully. Id. Second, a  
18 "vague law impermissibly delegates basic policy matters to  
19 policemen, judges, and juries" allowing for "arbitrary and  
20 discriminatory application." Id. at 108-09. Finally, a vague  
21 law touching on rights protected by the First Amendment  
22 inhibits the exercise of those rights; uncertainty can cause  
23 speakers to say less. Id. at 109. Therefore, when First  
24 Amendment interests are at stake, an even greater degree of  
25 specificity is required. Buckley v. Valeo, 424 U.S. 1, 77  
26 (1976); Bullfrog Films, Inc. v. Wick, 847 F.2d 502, 512 (9th

1 Cir. 1988) (citing N.A.A.C.P. v. Button, 371 U.S. 415, 432-33  
2 (1963)). However, for a claim of facial vagueness to survive,  
3 the deterrent effect of the statute on protected expression  
4 must be "real and substantial" and not easily narrowed by a  
5 court. Young v. American Mini Theaters, Inc., 427 U.S. 50, 60  
6 (1976).

7 Plaintiff asserts that the AECA is impermissibly vague in  
8 that the statute lacks standards sufficient to guide its  
9 application by administrators, thus giving rise to arbitrary  
10 and discriminatory enforcement. Plaintiff also charges  
11 vagueness with respect to the ITAR terms "defense articles,"  
12 "defense services," "technical data," "public domain," and  
13 "export." Defendants dispute each of these contentions.

14 Plaintiff's argument that the AECA itself is vague is best  
15 characterized as an issue under the APA, which, if it still  
16 appears necessary to address, the court defers to another  
17 day.<sup>14</sup> Grayned, on which plaintiff relies for support, was  
18 concerned with the delegation of policy matters to police,  
19 judges and juries, entities not normally entrusted with policy  
20 decisions. In contrast, the AECA, like many federal statutes,  
21 delegates to federal agencies and departments the  
22 responsibility of making more detailed policy decisions in the  
23 course of promulgating regulations under the law. Here, one  
24 set of policy makers has entrusted other policy makers with  
25 sensitive policy issues. This was not the situation in Grayned  
26 and it does not implicate the vagueness doctrine.

1            Plaintiff also argues that the ITAR is impermissibly vague  
2            in that the definitions of "defense articles," "defense  
3            services," and "technical data" all encompass the others.  
4            Specifically, a defense article "means any item or technical  
5            data designated in §121.1 of this subchapter." 22 C.F.R. §  
6            120.6 (emphasis added). Technical data, as defined in the ITAR  
7            and by the court in Edler, is information required for the  
8            manufacture or operation of defense articles or information  
9            directly relating to defense articles. 22 C.F.R. § 120.10.  
10           The definition of defense services distinguishes between  
11           defense articles and technical data. 2 C.F.R. § 120.9.  
12           Defendants argue that technical data is defined separately in  
13           the ITAR and in a manner that distinguishes it from actual  
14           commodities treated as defense articles such that it is not a  
15           defense article itself. However, the exact language of the  
16           ITAR does not comport with defendants' characterization of it.  
17           The definition of defense articles includes technical data,  
18           which according to its own definition can only be understood in  
19           relation to defense articles. To say this is vague would be  
20           generous, but it need not be voided for it is easily cured.  
21           The phrase "or technical data" as well as the third sentence of  
22           the definition referring to technical data must be removed from  
23           the definition of defense article. Accordingly, items listed  
24           on the USML are defense articles and information relating  
25           directly to them are technical data. Read in this way, the  
26           three terms are not impermissibly vague.

1 Plaintiff next claims that the exemptions to the  
2 definition of technical data are vague, specifically the public  
3 domain exemption and the academic exemption. Plaintiff claims  
4 that the public domain exemption presents a classic catch-22 in  
5 which items that are already published are exempted but  
6 publishing an item can invite prosecution under the ITAR. The  
7 definition of public domain includes "information which is  
8 published and which is generally accessible or available to the  
9 public" through a number of channels, including newsstands,  
10 bookstores, libraries and subscriptions. 22 C.F.R. §  
11 120.11(a) (1) - (7). With respect to subsections (1) through (7),  
12 this exemption is fairly well-defined, and not vague. It gives  
13 a person of ordinary intelligence concrete examples of the  
14 kinds of items that are in the public domain. The catch-22  
15 plaintiff complains of is inherent in a licensing scheme rather  
16 than in the statute's definitional terms and as such, has been  
17 addressed in the court's discussion of prior restraint.

18 However, the same cannot be said of section 120.11(a) (8),  
19 which contains the exemption for information available to the  
20 public "through fundamental research in science and  
21 engineering". 22 C.F.R. § 120.11(a) (8). This subsection, like  
22 the academic exemption which exempts "general scientific,  
23 mathematical or engineering principles" commonly taught in  
24 schools and universities, 22 C.F.R. § 120.10(a) (5), does not  
25 give people, particularly those of arguably extraordinary  
26 intelligence who are themselves engaged in the applied

1 sciences, "a reasonable opportunity to know what is  
2 prohibited". Grayned, 408 S.Ct. at 108. Given the direct  
3 application of these exemptions to First Amendment protections,  
4 the uncertainty created in scientists about what speech is  
5 subject to regulation under the ITAR is unacceptable.

6 For example, fundamental research is defined as "basic and  
7 applied research in science and engineering where the resulting  
8 information is ordinarily published and shared broadly within  
9 the scientific community". 22 C.F.R. § 120.11(a)(8). As  
10 defendants themselves repeatedly attest, cryptographic  
11 algorithms and theory are often published in scientific  
12 journals. Crowell Decl., Exhs. 1-10; Joint Statement of  
13 Undisputed Facts ¶ 9. However, cryptographic algorithms are  
14 also covered by Category XIII(b) of the USML. Given these two  
15 facts, it would be hard for scientists to discern when their  
16 work was a defense article and when it was wholly exempt from  
17 the ITAR without going through a CJ determination before any  
18 effort at publication. In fields of applied science, what is  
19 commonly taught in universities may well overlap with what the  
20 government might choose to regulate. In this instance the  
21 deterrent effect on protected expression appears both real and  
22 substantial. Young v. American Mini Theaters, Inc., 427 U.S.  
23 at 60. These academic exemptions from the definition of  
24 technical data, 22 C.F.R. §§ 120.10(a)(5) & 120.11(a)(8), are  
25 accordingly void for vagueness.

26 Lastly, plaintiff challenges the term "export" as vague

1 for two reasons. First, because it encompasses publishing and  
2 second, because what constitutes an export depends on whether  
3 an item is defined as a defense article or as technical data  
4 and those definitions are themselves vague. The first issue is  
5 more properly one of overbreadth and will be addressed below.  
6 The second is clarified by the modifications made by the court  
7 to the definition of defense article.

8 Export is defined as "[s]ending or taking a defense  
9 article out of the United States in any manner", 22 C.F.R. §  
10 120.17(a) (1), and as "[d]isclosing (including oral or visual  
11 disclosure) or transferring technical data to a foreign person,  
12 whether in the United States or abroad". 22 C.F.R. §  
13 120.17(a) (4). The NRC Report states that "[t]here is  
14 uncertainty about what specific act constitutes the 'export' of  
15 software products with encryption capabilities." NRC Report at  
16 4-16. The Report gives the example of uploading an encryption  
17 product to an Internet site in the United States where it can  
18 be downloaded by a user in another country, and asks if the  
19 exportation is in the upload or the download. NRC Report at 4-  
20 16, 4-17. This example appears to point out the uncertainty in  
21 what acts can actually be prosecuted under the ITAR more than  
22 any uncertainty in the definition of export. It seems  
23 reasonably clear that uploading an item to an Internet site  
24 that can be accessed in a foreign country constitutes "sending"  
25 a defense article out of the country. The court does not find  
26 that the term "export" is impermissibly vague.

1 B. Overbreadth

2 In a facial challenge to a law on grounds of overbreadth,  
3 a court must first "determine whether the enactment reaches a  
4 substantial amount of constitutionally protected conduct. If  
5 it does not, then the overbreadth challenge must fail."  
6 Village of Hoffman Est. v. Flipside, Hoffman Est., 455 U.S.  
7 489, 494 (1982).

8 Facial overbreadth is concededly "strong medicine"  
9 employed as a last resort when a limiting construction cannot  
10 be applied to a statute. Broadrick v. Oklahoma, 413 U.S. 601,  
11 613 (1973). In Members of the City Council of Los Angeles v.  
12 Taxpayers for Vincent, 466 U.S. 789 (1984), the Court noted  
13 that "where the statute unquestionably attaches sanctions to  
14 protected conduct, the likelihood that the statute will deter  
15 that conduct is ordinarily sufficiently great to justify an  
16 overbreadth attack." Id. at 801 n.19 (citing Erznoznik v. City  
17 of Jacksonville, 422 U.S. 205 (1975)). However, the Court also  
18 clarified the application of substantial facial overbreadth,  
19 saying there must be a "realistic danger that the statute  
20 itself will significantly compromise recognized First Amendment  
21 protections of parties not before the Court . . . ." Id. at  
22 801. Merely being able to conceive of "some impermissible  
23 applications of a statute" is insufficient. Id. at 800.

24 Defendants argue that although the traditional rules of  
25 standing are modified in the context of an overbreadth  
26 challenge on First Amendment grounds, Brockett v. Spokane

1 Arcades, Inc., 472 U.S. 491, 503 (1984) (noting cases holding  
2 that one whose own speech is validly prohibited by statute may  
3 still challenge statute facially because it threatens others  
4 not before the court), that is not the case where the party  
5 before the court seeks to engage in protected speech that the  
6 statute purports to punish. In that case, there is "no want of  
7 a proper party to challenge the statute, no concern that an  
8 attack on the statute will be unduly delayed or protected  
9 speech discouraged." Brockett, 472 U.S. at 504. Accordingly  
10 defendants assert that because plaintiff cannot show a  
11 significant difference between his claims and those of third  
12 parties, the court must consider the overbreadth challenge as  
13 applied to plaintiff. Plaintiff disputes this by citing cases  
14 emphasizing that if a statute's overbreadth is substantial and  
15 its chilling effect significant, the entire statute may be  
16 invalidated to protect the First Amendment. Lind v. Grimmer,  
17 30 F.2d 115, 1122 (9th Cir. 1994), cert. den sub nom. Want v.  
18 Lind, 115 S.Ct. 902 (1995) (distinguishing cases in which the  
19 only unconstitutional application was the one directed at the  
20 party before the court and where the chilling effect could be  
21 obviated by partial invalidation); see also Board of Airport  
22 Comm'rs of Los Angeles v. Jews for Jesus, Inc., 482 U.S. 569,  
23 573-74 (1987).

24 The court need not resolve this dispute over standing  
25 because the issues left unresolved are few, and for those that  
26 remain the nature of the challenge will not make a difference.

1 The First Amendment does not "render inapplicable the rule that  
 2 a federal court should not extend its invalidation of a statute  
 3 further than is necessary to dispose of the case before it."  
 4 Brockett, 472 U.S. at 502 (citation omitted). The court is  
 5 mindful of that admonition. It has ruled on Category XIII(b)  
 6 and technical data generally under prior restraint analysis; it  
 7 has offered a curing instruction for the definition of "defense  
 8 articles" and has invalidated the academic exemptions to  
 9 technical data on vagueness grounds. All that remains are  
 10 plaintiff's claims that the definition of export is overbroad  
 11 and that the entire ITAR scheme is overbroad in that it assumes  
 12 that all foreigners are terrorists. The latter strikes the  
 13 court as patently absurd. The former can be disposed of  
 14 quickly.

15 As noted above, "export" is defined with respect to  
 16 defense articles as "[s]ending or taking a defense article out  
 17 of the United States in any manner", 22 C.F.R. § 120.17(a)(1).  
 18 With respect to technical data it means "[d]isclosing  
 19 (including oral or visual disclosure) or transferring technical  
 20 data to a foreign person, whether in the United States or  
 21 abroad". 22 C.F.R. § 120.17(a)(4). The provision governing  
 22 the exportation of defense articles is clearly aimed mainly at  
 23 conduct--at shipping tanks, missiles and the like abroad. Yet  
 24 in regulating cryptographic software it also sweeps in speech.  
 25 While the overbreadth of the provision in this respect is real,  
 26 the court cannot say that it is "substantial as well, judged in

1 relation to the statute's plainly legitimate sweep."  
2 Broadrick, 413 U.S. at 615. With respect to the export of  
3 technical data, this court is again bound by Edler regardless  
4 of whether it agrees with that disposition. There the Ninth  
5 Circuit added a scienter requirement to the prohibition against  
6 exporting technical data in order to cure the overbreadth  
7 problem. Edler, 579 F.2d at 521.

8 Accordingly, neither the definition of export nor the ITAR  
9 scheme as a whole is unconstitutionally overbroad.

10  
11 III. Administrative Procedures Act

12 In light of the foregoing, the court finds it unnecessary  
13 to reach the claims brought by plaintiff under the APA.

14  
15 IV. Preliminary Injunction

16 Plaintiff also seeks a preliminary injunction to enjoin  
17 the government from prosecuting him under the ITAR and AECA for  
18 his teaching activities. Plaintiff plans to teach a class on  
19 the theory and practice of cryptography at the University of  
20 Illinois at Chicago beginning in January of 1997. Plaintiff  
21 believes that foreign students may take his class and intends  
22 to post class materials, including cryptographic algorithms, on  
23 the University's Internet website for students to access.

24 Defendants assert that a preliminary injunction is  
25 unwarranted because teaching a class on cryptography does not  
26 violate the regulations. They also argue that the motion for a

1 preliminary injunction is merely an attempt by plaintiff to  
2 circumvent export controls by distributing cryptographic  
3 software abroad in the name of academic freedom.

4 The court notes that an injunction appears hasty given the  
5 relative positions of the parties. The government seems to  
6 suggest that teaching a class on cryptography, regardless of  
7 the nationality of the students, is not the problem; the  
8 concern is with posting material on the Internet without  
9 limiting access. Assuming the government is sincere about its  
10 limited objections and that plaintiff could easily limit access  
11 to the class material he posts so that it is not available  
12 internationally, it is not clear why the parties could not  
13 enter into a stipulation.

14 In view of the fact that the court has ruled on the merits  
15 and has found certain provisions of the ITAR invalid, plaintiff  
16 cannot be prosecuted under those provisions absent reversal on  
17 appeal. Therefore, at this time there is no immediate threat  
18 of injury and no need to rule on the preliminary injunction.<sup>15</sup>  
19 The motion for a preliminary injunction is denied without  
20 prejudice. If plaintiff is threatened with prosecution, he may  
21 return to this court and renew the motion.

22 //

23 //

24 //

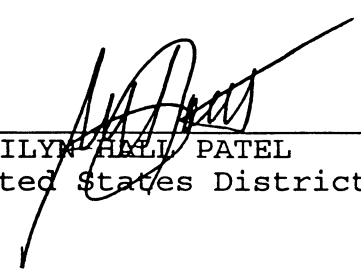
1 CONCLUSION

2 For the reasons set forth above, IT IS HEREBY ORDERED that  
3 plaintiff's motion for summary judgment is GRANTED in part and  
4 DENIED in part. Defendants' motion for summary judgment is  
5 likewise GRANTED in part and DENIED in part. Plaintiff's  
6 motion for a preliminary injunction is DENIED without  
7 prejudice.

8  
9 IT IS SO ORDERED.

10  
11 Dated:

Dec. 6, 1996

  
\_\_\_\_\_  
MARILYN HILL PATEL  
United States District Judge

ENDNOTES

1

1, 2 Some of the information in this section is taken directly from the court's previous opinion in this action, Bernstein v. United States Dept. of State, 922 F. Supp. 1426, 1428-30 (N.D. Cal. 1996), and is repeated here for its relevance to the present motion. Additional information comes from the parties' submissions or other sources as indicated.

2, 5 In symmetric cryptography the encryption key is the same as the decryption key. Asymmetric, or public-key, cryptography uses different keys for encryption and decryption and generally only the encryption key is disclosed.

3, 8 Source code is the text of a source program and is generally written in a high-level language that is two or more steps removed from machine language which is a low-level language. High-level languages are closer to natural language than low-level languages which direct the functioning of the computer. Source code must be translated by way of a translating program into machine language before it can be read by a computer. The object code is the output of that translation. It is possible to write a source program in high-level language without knowing about the actual functions of the computer that carry out the program. Encyclopedia of Computer Science 962, 1263-64 (Anthony Ralston & Edwin D. Reilly eds., 3d ed. 1995)

14, 4 The parties disagree about whether the computer code submitted by plaintiff to the State Department is technically "software." The court notes that 22 C.F.R. § 121.8(f) defines "software" for the purposes of the AECA. That definition is descriptive of content, however, and does not define the actual format or physical form of the software. However, 22 C.F.R. § 120.4(d)(2), pertaining to the commodity jurisdiction procedure, contains the note that for the purposes of software, "form denotes language, language level and media" while the function is "the action or actions it is designated to perform." For the purposes of this motion the court need not resolve this issue since regardless of Snuffle's exact form, it appears to meet the definitions contained in the statute and the ODTIC has subjected it to the licensing requirements.

5, 22 The CJ request of July 15, 1993, refers to the items as DJBCJF-2, DJBCJF-3, DJBCJF-4, DJBCJF-5, and DJBCJF-6 without distinguishing information. Complaint Exh. D.

6, 24 Plaintiff contends that the CJ process, the registration and fee system, the licensing system and the recordkeeping mandate all function as a prior restraint on speech. For the purpose of this motion, this is overkill. Defendants do not dispute the licensing system for defense articles. As defendants point out, the CJ process is voluntary, although it appears to function as a

27

28

pre-licensing system. The court will analyze the ITAR mainly with respect to the licensing system itself.

7.<sup>2</sup> One might make the argument that encryption software could be validly regulated for its "secondary effects," much like adult theaters were in Young v. American Mini-Theaters, Inc., 427 U.S. 50 (1975), and Renton v. Playtime Theaters, Inc., 475 U.S. 41 (1986), where the Supreme Court upheld zoning ordinances aimed at the secondary effects of such theaters in the surrounding community. However, the secondary effects rationale has never been extended beyond sexually explicit speech. See Boos v. Barry, 485 U.S. 312 (1988) (refusing to apply the rationale to political speech).

8. The court recognizes that the vendors the NRC Report discusses have different speech interests in cryptography than academic scientists. However, the Report is nonetheless valuable for its up-to-date insights into the actual implementation of the ITAR export controls over cryptographic products.

9. The NRC Report states that the recent lawsuits in this area, including the instant one, "suggest quite strongly that the traditional national security paradigm of export controls on cryptography (one that is biased toward denial rather than approval) is stretched greatly by current technology. Put differently, when the export control regime is pushed to an extreme, it appears manifestly ridiculous." NRC Report at 4-33.

10. This is like the controversy surrounding Bruce Schneier's book, Applied Cryptography, which was the subject of litigation similar to the present action. See Karn v. United States Dept. of State, 925 F. Supp. 1 (D.D.C. 1996). The book contained source code for cryptography as well as a disk containing the identical source code. Karn received permission to export the book but not the disk. The NRC Report commented on the general dismay with which the academic cryptography community greeted this decision, repeating their quip: "They think terrorists can't type?" NRC Report at 4-48.

11. Also suggestive of the confusion surrounding application of this provision is the manner in which the ODC handled the CJ determination of plaintiff's paper. Based on this court's understanding of the correspondence between the ODC and Bernstein, the paper was initially determined to be on the USML. See Bernstein, 922 F. Supp. at 1434. Although the ODC claims this was because Bernstein presented his application in a confusing manner, it still took nearly two years for the ODC to determine only that the paper did not "appear" to be technical data. In a letter sent to plaintiff since the court issued its opinion, the ODC clarified that the paper was not technical data.

27

28

12. In an August 29, 1978 letter to Colonel Kay in the Office of Science and Technology Policy concerning the then recent decision in Edler, the Office of Legal Counsel stated that while the Ninth Circuit's decision is helpful in resolving First Amendment issues with respect to blueprints and similar types of technical data used as a basis for producing military equipment, we do not believe that it either resolves the First Amendment issues presented by restrictions on the export of cryptographic ideas or eliminates the need to reexamine the ITAR.

Tjen Decl., Exh. D at 2.

13. The court disagrees with plaintiff's contention that the elimination of judicial review allows for reconsideration of Edler. The judicial review provision, which was added in 1989, does not address licensing decisions but precludes judicial review only as to the designation of items as defense articles or services. 22 U.S.C. § 2778(h).

14. This set of summary judgment motions was set specifically to address First Amendment issues.

15. In order to establish injury plaintiff need not "expose himself to actual arrest or prosecution . . ." Steffel v. Thompson, 415 U.S. 452, 459 (1974). However, neither can the threat of prosecution be speculative. Id.; Caribbean Marine Servs. Co., Inc. v. Baldrige, 844 F.2d 668, 675 (9th Cir. 1988).

United States District Court  
of California  
San Diego

15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

