945 F.Supp. 1279
United States District Court,
N.D. California.

Daniel J. BERNSTEIN, Plaintiff,

v.

UNITED STATES DEPARTMENT OF STATE et al., Defendants.

No. C–95–0582 MHP.
Dec. 9, 1996.

Mathematician sought declaratory and injunctive relief against enforcement of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) on the grounds that they were unconstitutional on their face and as applied to mathematician's cryptographic computer source code. On cross-motions for summary judgment, the District Court, Patel, J., held that: (1) licensing requirements for speech relating to encryption of computer software constituted unlawful prior restraint; (2) definitions of terms in ITAR, including "defense articles," "defense services," and "technical data," were not vague; (3) exemptions from term "technical data" for academic items, but not for items in public domain, were impermissibly vague; (4) term "export" was not vague; and (5) neither ITAR scheme as whole nor definition of "export" were overbroad.
Ordered accordingly.

MEMORANDUM AND ORDER

PATEL, District Judge.

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. §§ 120.1–130.7 (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 on speech in violation of the First Amendment.
Having considered the parties' arguments and submissions, and for the reason set forth below, the court enters the following memorandum and order.
BACKGROUND[1]

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

I. *Cryptography*

Encryption basically involves running a readable message known as "plaintext" through a computer program that translates the message according to an equation or algorithm into unreadable "ciphertext." Decryption is the translation back to plaintext when the message is received by someone with an appropriate "key." The message is both encrypted and decrypted by compatible keys.[2] The uses of cryptography are far-ranging in an electronic age, from protecting personal messages over the Internet and transactions on bank ATMs to ensuring the secrecy of military intelligence. In a prepublication copy of a report done by the National Research Council ("NRC") at the request of the Defense Department on national cryptography policy, the NRC identified four major uses of cryptography: ensuring data integrity, authenticating users, facilitating nonrepudiation (the linking of a specific message with a specific sender) and maintaining confidentiality. Tien Decl., Exh. E, National Research Council, National Academy of Sciences, *Cryptography's Role in Securing the Information Society* C–2 (Prepublication Copy May 30, 1996) (hereinafter "NRC Report").

Once a field dominated almost exclusively by governments concerned with protecting ***1283** their own secrets as well as accessing information held by others, the last twenty years has seen the popularization of cryptography as industries and individuals alike have increased their use of electronic media and have sought to protect their electronic products and communications. NRC Report at vii. As part of this transformation, cryptography has also become a dynamic academic discipline within applied mathematics. Appel Decl. at 5; Blaze Decl. at 2.

As a graduate student, Bernstein developed an encryption algorithm he calls "Snuffle." He describes Snuffle as a zero-delay private-key encryption system. Complaint Exh. A. Bernstein has articulated his mathematical ideas in two ways: in an academic paper in English entitled "The Snuffle Encryption System," and in "source code" written in "C", a high-level computer programming language,[3] detailing both the encryption and decryption, which he calls "Snuffle.c" and "Unsnuffle.c", respectively. Once source code is converted into "object code," a binary system consisting of a series of 0s and 1s read by a computer, the computer is capable of encrypting and decrypting data.[4]

II. *Statutory and Regulatory Background*

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

The International Traffic in Arms Regulations, 22 C.F.R. §§ 120.1–130.17, were promulgated by the Secretary of State, who was authorized by executive order to implement the AECA. The ITAR is administered primarily within the Department of State by the Director of the Office of Defense Trade Controls ("ODTC"), Bureau of Politico–Military Affairs. The ITAR allows for a "commodity jurisdiction procedure" by which the ODTC determines if an article or service is covered by the USML when doubt exists about an item. 22 C.F.R. § 120.4(a). Also contained in the ITAR are the licensing requirements for defense articles, 22 C.F.R. § 123, and technical data, 22 C.F.R. § 125.

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

A "defense article" is defined by the ITAR as any item or technical data that has been designated in the USML. 22 C.F.R. § 120.6. A "defense service" is any assistance rendered to a foreign person in the United States or abroad in the development or use ***1284** of a defense article, 22 C.F.R. § 120.9(a)(1), or the furnishing of technical data to a foreign person, 22 C.F.R. § 9(a)(2).

"Technical data" is perhaps the most confusing category of items regulated by the ITAR since it is defined separately and *in relation to* defense articles, 22 C.F.R. § 120.10, but is also defined *as* a defense article when it is covered by the USML. *See* 22 C.F.R. § 120.6. It generally covers information "which is required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles." 22 C.F.R. § 120.10. It also encompasses software directly related to defense articles. 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 exceptions apply only to technical data and not to defense articles.

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

III. *Plaintiff's Commodity Jurisdiction Determinations*

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

Plaintiff and ODTC exchanged copious and contentious correspondence regarding the licensing requirements during the spring of 1993. Still unsure if his academic paper had been included in the ODTC CJ determination of August 20, 1992, Bernstein submitted a second CJ request on July 15, 1993, asking for a separate determination for each of five items. Lowell Decl., Exh. 17. According to plaintiff these items were 1) the paper, "The Snuffle Encryption System," 2) Snuffle.c, 3) Unsnuffle.c, 4) a description in English of ***1285** how to use Snuffle, and 5) instructions in English for programming a computer to use Snuffle.[5] On October 5, 1993 the ODTC notified Bernstein that *all* of the referenced items were defense articles under Category XIII(b)(1). Complaint Exh. E. By letter dated June 29, 1995, after plaintiff had initiated this action, the ODTC clarified that its CJ determinations pertained only to Snuffle.c and Unsnuffle.c, which it had determined to be a defense article on the USML. Lowell Decl., Exh. 21 at 1. The ODTC further noted that the two items of explanatory information fell within the definition of technical data but that the paper, "The Snuffle Encryption System," did "not appear to meet the definition of technical data." Lowell Decl., Exh. 21 at

2. The June 29 letter also explains the public domain exception to technical data without drawing a conclusion about the applicability of that exception to the explanatory information.

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

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

LEGAL STANDARD

Under Federal Rule of Civil Procedure 56, summary judgment shall be granted "against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial ... since a complete failure of proof concerning an essential element of the nonmoving party's case necessarily renders all other facts immaterial."*Celotex Corp. v. Catrett,* 477 U.S. 317, 322–23, 106 S.Ct. 2548, 2552, 91 L.Ed.2d 265 (1986); *see also T.W. Elec. Serv. v. Pacific Elec. Contractors Ass'n,* 809 F.2d 626, 630 (9th Cir.1987) (the nonmoving party may not rely on the pleadings but must present significant probative evidence supporting the claim); *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 248, 106 S.Ct. 2505, 2510, 91 L.Ed.2d 202 (1986) (a dispute about a material fact is genuine "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.").

The court's function, however, is not to make credibility determinations, *Anderson,* 477 U.S. at 249, 106 S.Ct. at 2510–11, and the inferences to be drawn from the facts must be viewed in a light most favorable to the party opposing the motion. *T.W. Elec. Serv.,* 809 F.2d at 631.

Where as here, the question is purely a legal one involving no disputes of material fact, the matter is appropriately handled on a motion for summary judgment.

DISCUSSION

Plaintiff contends that the licensing scheme under the ITAR imposes an unconstitutional prior restraint on cryptographic speech, whether that speech is defined as a defense article or technical

data. Plaintiff further maintains that a number of terms make the ITAR vague and overbroad in violation of the First Amendment.

Defendants argue that the ITAR, insofar as it regulates cryptographic software, is content ***1286** neutral and easily survives intermediate scrutiny under the First Amendment. In addition, defendants aver that the technical data provisions do not regulate scientific or academic speech and therefore do not act as a prior restraint on speech. Finally, defendants contend that plaintiff's overbreadth claim, vagueness claim and his claims under the Administrative Procedure Act ("APA") are without merit.

Both parties sizable briefs in support of their motions for summary judgment are notable for the contrast of their approaches. Plaintiff, for his part, argues that the provisions of the ITAR at issue violate numerous conceivable—and a few inconceivable—First Amendment doctrines. Defendants' arguments, in contrast, while steering closer to traditional first amendment analysis, are notable for the conspicuous absence of discussion of the prior restraint doctrine.

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

I. *Prior Restraint*

A. *Analytical Framework*

As the Supreme Court has stated, in determining the extent of the constitutional protection afforded by the guarantees of the First Amendment, "it has been generally, if not universally, considered that it is the chief purpose of the guaranty to prevent previous restraints upon publication." *Near v. Minnesota,* 283 U.S. 697, 713, 51 S.Ct. 625, 630, 75 L.Ed. 1357 (1931). It is for this reason that the Court has held: "Any prior restraint on expression comes to this Court with a 'heavy presumption' against its constitutional validity." *Organization for a Better Austin v. Keefe,* 402 U.S. 415, 419, 91 S.Ct. 1575, 1578, 29 L.Ed.2d 1 (1971) (citations omitted).

1While prior restraints have often come in the form of judicial injunctions on publication, *see e.g., C.B.S. v. Davis,* 510 U.S. 1315, 114 S.Ct. 912, 127 L.Ed.2d 358 (1994); *New York Times Co. v. United States,* 403 U.S. 713, 91 S.Ct. 2140, 29 L.Ed.2d 822 (1971), they are also recognized in licensing schemes. *See e.g., FW/PBS, Inc. v. Dallas,* 493 U.S. 215, 110 S.Ct. 596, 107 L.Ed.2d 603 (1990);*Lakewood v. Plain Dealer Publishing Co.,* 486 U.S. 750, 108 S.Ct. 2138, 100 L.Ed.2d 771 (1988). Governments may impose valid time, place and manner restrictions when they are content neutral, narrowly tailored to serve a substantial governmental interest, and leave open alternative channels for communication. *See e.g., Clark v. Community for Creative Non–Violence,* 468 U.S. 288,

293, 104 S.Ct. 3065, 3068–69, 82 L.Ed.2d 221 (1984). However, “even if a government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not *condition* that speech on obtaining a license or permit from a government official in that official's boundless discretion.” *Lakewood,* 486 U.S. at 764, 108 S.Ct. at 2147.

2It is axiomatic that the First Amendment is more tolerant of subsequent criminal punishment of speech than it is of prior restraints on the same speech.

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

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

***1287** *Nebraska Press Ass'n v. Stuart,* 427 U.S. 539, 559, 96 S.Ct. 2791, 2803, 49 L.Ed.2d 683 (1976). While the Supreme Court has consistently rejected the idea that a prior restraint can never be employed, *id.* at 570, 96 S.Ct. at 2808, it nonetheless begins with a presumption of invalidity. The danger inherent in prior restraints is largely procedural, in that they bypass the judicial process and locate in a government official the delicate responsibility of passing on the permissibility of speech. *See Freedman v. Maryland,* 380 U.S. 51, 58, 85 S.Ct. 734, 738–39, 13 L.Ed.2d 649 (1965) (holding that “a noncriminal process which requires the prior submission of a film to a sensor avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system”.) *Freedman* sets forth three procedural safeguards that have been used by the Supreme Court to examine licensing schemes: 1) any prior restraint to judicial review can only be imposed for a brief and specified period during which the status quo prevails; 2) expeditious judicial review must be available; and 3) the censor must bear the burden of going to court to suppress speech and once there bears the burden of proof. *FW/PBS,* 493 U.S. at 227, 110 S.Ct. at 605–06 (citing *Freedman,* 380 U.S. at 58–60, 85 S.Ct. at 738–40).

3When the risks associated with unbridled licensing schemes are present to a significant degree, “courts must entertain an immediate facial attack on the law.” *Lakewood,* 486 U.S. at 759, 108 S.Ct. at 2145.

B. *Analysis*

Plaintiff argues that the CJ process, the registration and fee system and the licensing system under the ITAR all act as prior restraints on his ability to communicate and publish both his source code and its accompanying technical data. Additionally, plaintiff contends that by failing to meet the procedural requirements of *Freedman* the ITAR scheme violates the First Amendment.

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

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

1. *Category XIII(b) of the USML*

4A couple of preliminary observations are in order. The first concerns the nature of the speech involved. Plaintiff cites *Hurley v. Irish–American Gay Group of Boston,* —— U.S. ——, 115 S.Ct. 2338, 132 L.Ed.2d 487 (1995), to assert that the First Amendment prevents compelled speech and *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334, 115 S.Ct. 1511, 131 L.Ed.2d 426 (1995), in support of its protection of anonymous speech. Based on these cases plaintiff advances the novel proposition that the First Amendment also includes the right to speak confidentially, and thus, encryption is deserving of protection because it facilitates private communication. It is unnecessary, and this court is unwilling, to reach this issue. The court reiterates its previous conclusion that source code is speech.*Bernstein,* 922 F.Supp. at 1436. Software relating to encryption is simply a topic of speech employed by some scientists involved in applied research. Hence, Snuffle is speech afforded the full protection of the First Amendment not because it enables encryption, but because it is itself speech.

5Second, defendants assume that if the ITAR export controls do not restrict the content of protected speech they are not a prior restraint. This misunderstands the prior restraint analysis. If a licensing scheme does not employ sufficient procedural safeguards, it must be invalidated not because it is necessarily content based but because it bestows on a government official substantial power to discriminate based on the content of the speech or to burden speech by delaying a licensing decision. *Lakewood,* 486 U.S. at 759, 108 S.Ct. at 2145; *see also FW/PBS,* 493 U.S. at 229, 110 S.Ct. at 606–07 (plurality opinion) (finding that under ***1288** the ordinance at issue the city did not pass judgment on the content of the protected speech but had an indefinite amount of time to issue license).

Category XIII(b) of the USML—directed as it is to cryptographic software where software includes logic flows, algorithms and source code—covers speech protected by the First Amendment. Defendants do not dispute that the State Department requires a license to export items covered by Category XIII(b).[6] Furthermore, exportation as defined by the ITAR would appear to include publication where publication, such as posting software on the Internet or distributing it freely among colleagues, could be said to be tantamount to sending it out of the United States "in any manner". 22 C.F.R. § 120.17(a)(1).

6A facial challenge on the basis of prior restraint will lie where a law has a "close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of identified censorship risks." *Lakewood,* 486 U.S. at 759, 108 S.Ct. at 2145. In *Lakewood,* a newspaper challenged a city ordinance which required annual permits for newsracks on public property and gave the mayor authority to grant or deny applications for those permits. The Court contrasted laws that are directed at expression, such as the one governing the circulation of newspapers, with laws of general applicability not aimed at conduct commonly associated with expression, such as a law requiring building permits. *Id.* at 760–61, 108 S.Ct. at 2145–46. The former risks self-censorship on the part of those applying for permits and censorship on the part of the decisionmaker. The latter rarely do.

7While, as defendants assert, the bulk of the ITAR scheme may well be viewed as a law of general applicability not aimed at expression but at controlling the spread of defense-related commodities abroad, the same cannot be said of Category XIII(b) of the Munitions List. Category XIII(b) is directed very specifically at applied scientific research and speech on the topic of encryption. That it regulates encryption in the interest of national security does not alone justify a prior restraint. In *New York Times Co.,* 403 U.S. at 714, 91 S.Ct. at 2141–42, the Supreme Court invalidated a prior restraint on classified material that had been enjoined in the interests of national security. While that case inspired nine separate opinions on the propriety of enjoining publication of the Pentagon Papers in The New York Times and The Washington Post, a majority of Justices found national security, without more, too amorphous a rationale to abrogate the protections of the First Amendment. *See id.* at 719, 91 S.Ct. at 2144 (Black, J. and Douglas, J., concurring). Justice Brennan concluded that the First Amendment's ban on prior restraints could only be overridden in time of war, *id.* at 726, 91 S.Ct. at 2147–48 (Brennan, J. concurring) (citing *Schenck v. United States,* 249 U.S. 47, 39 S.Ct. 247, 63 L.Ed. 470 (1919)), and even then, according to Justice Stewart, only when disclosure would "surely result in direct, immediate, and irreparable damage to our Nation or its people." *Id.* at 730, 91 S.Ct. at 2149 (Stewart, J. and White, J. concurring). Under such an exacting standard, defendants' interests here, in being able to break foreign encryption and conduct adequate surveillance in "furtherance of world peace and the security and foreign policy of the United States," 22 U.S.C. § 2778(a)(1), are clearly insufficient without more.

However, even though in *form* Category XIII(b) aims at speech, it is arguable—and defendants assert—that its *purpose* is content neutral. Yet the very nature of the technology blurs the distinction between these two ways of understanding the constitutionality of a regulation. With respect to encryption, the stronger the cryptographic algorithm, the better the science and the more noteworthy the academic speech, but also the more powerful are its effects and ***1289** therefore the greater the interest in government regulation.[7]

However, even if the court were to determine that the regulatory purpose behind Category XIII(b) was content neutral that would not resolve the issue. The plurality opinion in *FW/PBS* suggests that even an otherwise valid licensing scheme must still contain adequate procedural safeguards in order to be constitutional. There Justice O'Connor, joined by Justices Stevens and Kennedy, stated: Because we conclude that the city's licensing scheme lacks adequate procedural safeguards, we do not reach the issue decided by the Court of Appeals whether the ordinance is properly viewed as a content-neutral time, place, and manner restriction aimed at secondary effects arising out of the sexually oriented businesses.

FW/PBS, 493 U.S. at 223, 110 S.Ct. at 603. Thus, the court turns to the procedural safeguards afforded by the ITAR.

As noted above, the Court in *FW/PBS* read *Freedman* to hold that for a licensing scheme to be constitutional, 1) the licensor must make the licensing decision within a specific and reasonable period of time; 2) there must be prompt judicial review; and 3) the censor must bear the burden of going to court to uphold a licensing denial and once there bears the burden of justifying the denial. *FW/PBS,* 493 U.S. at 227–28, 110 S.Ct. at 605–06 (citing *Freedman,* 380 U.S. at 58–60, 85 S.Ct. at 738–40).

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

According to the NRC Report, some of the problems that standardless discretion invite have been realized among commercial vendors of cryptographic products.[8] The Report notes, for example, that

virtually all industry representatives testified that product development was inhibited and trust eroded by the unpredictability of USML licensing, a lengthy licensing process and the lack of an independent adjudicating forum in which to appeal negative licensing decisions. NRC Report at 4–14, 4–15, 4–17. In addition, the ***1290*** risk of discriminatory treatment associated with standardless licensing schemes was reflected in the Report's comments that companies were reluctant to express their full dissatisfaction with the rules and implementation of export controls over cryptographic products for fear that "any explicit connection between critical comments and their company might result in unfavorable treatment of a future application for an export license for one of their products." *Id.* at 4–29.

In *FW/PBS,* the Court declared that the first two safeguards required by *Freedman*—a time limit on the licensing decision and judicial review—were essential. *FW/PBS,* 493 U.S. at 228, 110 S.Ct. at 606. The third requirement that the censor bear the burdens of going to court and justifying its decision, it concluded, depended on the nature of the licensing scheme. Unlike the film censorship at issue in*Freedman,* the ordinance considered in *FW/PBS* did not entail "passing judgment on the content of any protected speech" and because the applicants were applying for a license of their entire business and not just a single film, the applicant had "every incentive ... to pursue a license denial through court." *Id.* at 230, 110 S.Ct. 607. For these reasons the plurality opinion concluded that the city was not required under the First Amendment to bear the burden of going to court or to bear the burden of proof once there. *Id.*

The ITAR licensing scheme for items listed in Category XIII(b) of the USML is more like the scheme in *Freedman* than *FW/PBS.* Here the relevant provision of the ITAR is directed at speech on a particular subject matter—cryptography. The Supreme Court has held that "the First Amendment's hostility to content-based regulation extends not only to a restriction on a particular viewpoint, but also to a prohibition of public discussion of an entire topic." *Burson v. Freeman,* 504 U.S. 191, 197, 112 S.Ct. 1846, 1850, 119 L.Ed.2d 5 (1992) (citing*Consolidated Edison Co. of N.Y. v. Public Service Comm'n of N.Y.,* 447 U.S. 530, 537, 100 S.Ct. 2326, 2333, 65 L.Ed.2d 319 (1980)). Furthermore, applicants must apply for a license for each item covered by Category XIII(b) and like the film distributor seeking approval of one film, may be deterred from challenging the licensing decision. For these reasons, this court concludes that the ITAR licensing scheme of cryptographic software is subject to all three procedural safeguards. Because it fails to provide for a time limit on the licensing decision, for prompt judicial review and for a duty on the part of the ODTC to go to court and defend a denial of a license, the ITAR licensing system as applied to Category XIII(B) acts as an unconstitutional prior restraint in violation of the First Amendment.

2. *The Technical Data Provision*

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

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

Defendants contend that *Edler* upheld a technical data provision that was considerably less friendly to First Amendment interests and that since then exemptions for academic research and discussion have been added and clarified. In addition to the exemptions of general scientific principles and fundamental research from the definition of technical data, defendants point to a number of scholarly articles on cryptographic theory that have been published free of ITAR licensing. Finally, the ODTC has indicated that it interprets the technical data provision in a manner consistent with *Edler*. 49 Fed.Reg. 47683 (Dec. 6, 1984).

***1291** In *Edler* the Ninth Circuit reviewed a conviction under the predecessor of the AECA for unlicensed exportation of technical data relating to a defense article on the USML. The technical data at issue in *Edler* related to a technique of tape wrapping with applications for missile components. In an appeal of his conviction, defendant challenged the statute and regulations on First Amendment grounds. After finding that "an expansive interpretation of technical data relating to items on the Munitions List could seriously impede scientific research and publishing and international scientific exchange," 579 F.2d at 519, the court went on to adopt a narrowing construction to save the statute. The court construed the statute and regulations to prohibit only the export of technical data "significantly and directly related to specific articles on the Munitions List." *Id.* at 521. In addition, when information could have both peaceful and military applications, the court added a scienter requirement that a defendant "must know or have reason to know that its information is intended for the prohibited use." *Id.* The Ninth Circuit concluded that as construed the statute and regulations were not overbroad and not a prior restraint on speech. *Id.*

This court has serious concerns about the viability of the *Edler* holding, particularly in light of advanced technologies such as cryptography and other applied sciences.[9] First, the Ninth Circuit's reasoning in *Edler* is not only twenty years old, but more importantly, it was made without the benefit of the Supreme Court's subsequent interpretation of *Freedman* and the procedural safeguards required of regulatory schemes that license speech. Second, the court notes with some concern that in practice the technical data provision appears to have been as confusing to those charged with implementing it as to those potentially regulated by it. The NRC Report notes that the rules governing technical data are particularly difficult to understand, pointing to the fact that a cryptographic algorithm that is not machine-readable is technical data while the same algorithm in

machine-readable form is a product.[10] The Report also provides excerpts from the only document it found in which the ODTC explains how the regulation of technical data relates to cryptography. NRC Report at 4–47. That 1980 document appears to be inconsistent with the *Edler* construction and suggests that the technical data provision could be used to directly regulate, and chill, academic discourse. It states: "The public is reminded that professional and academic presentations and informal discussions, as well as demonstrations of equipment, constituting disclosure of cryptographic technical data to foreign nationals are prohibited without the prior approval of this office." *Id.*[11] Lastly, defendants received between 1978 and 1984 three separate and extensive memoranda from the Department of Justice's Office of Legal Counsel, two regarding proposed revisions to the ITAR and one specifically addressing ***1292** the constitutionality of the ITAR restrictions on public cryptography. Tien Decl., Exhs. A–C. Each of them concludes, despite further revision and amendment to the ITAR, that the technical data provisions as they relate to academic and scientific speech are in violation of the First Amendment.[12]

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

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

II. *Vagueness and Overbreadth*

9The doctrines of vagueness and overbreadth have traditionally been viewed as related and similar doctrines by the Supreme Court. *Kolender v. Lawson*, 461 U.S. 352, 358 n. 8, 103 S.Ct. 1855, 1859 n. 8, 75 L.Ed.2d 903 (1983) (citations omitted). Vague or overbroad laws deter the constitutionally protected activity not only of the litigant, but of third parties not before the court, and for that reason can be challenged facially. *Grayned v. City of Rockford*, 408 U.S. 104, 114, 92 S.Ct. 2294, 2302, 33 L.Ed.2d 222 (1972). The court will consider each doctrine briefly with respect to those parts of the statute not already adjudicated. The court will not address Category XIII(b) but will consider other provisions and amendments to the technical data provision that were not in effect at the time of *Edler*.

A. *Vagueness*

1011Due process requires that laws clearly define their prohibitions. *Grayned*, 408 U.S. at 108, 92 S.Ct. at 2298–99. Vague laws are objectionable for multiple reasons. First, because they do not "give the person of ordinary intelligence a reasonable opportunity to know what is prohibited," they do not provide fair warning to those who wish to act lawfully. *Id.* Second, a "vague law impermissibly delegates basic policy matters to policemen, judges, and juries" allowing for "arbitrary and

discriminatory application." *Id.* at 108–09, 92 S.Ct. at 2299. Finally, a vague law touching on rights protected by the First Amendment inhibits the exercise of those rights; uncertainty can cause speakers to say less. *Id.* at 109, 92 S.Ct. at 2299. Therefore, when First Amendment interests are at stake, an even greater degree of specificity is required. *Buckley v. Valeo*, 424 U.S. 1, 77, 96 S.Ct. 612, 662–63, 46 L.Ed.2d 659 (1976); *Bullfrog Films, Inc. v. Wick*, 847 F.2d 502, 512 (9th Cir.1988) (citing *N.A.A.C.P. v. Button*, 371 U.S. 415, 432–33, 83 S.Ct. 328, 337–38, 9 L.Ed.2d 405 (1963)). However, for a claim of facial vagueness to survive, the deterrent effect of the statute on protected expression must be "real and substantial" and not easily narrowed by a court. *Young v. American Mini Theatres, Inc.*, 427 U.S. 50, 60, 96 S.Ct. 2440, 2447, 49 L.Ed.2d 310 (1976).

Plaintiff asserts that the AECA is impermissibly vague in that the statute lacks standards sufficient to guide its application by administrators, thus giving rise to arbitrary ***1293*** and discriminatory enforcement. Plaintiff also charges vagueness with respect to the ITAR terms "defense articles," "defense services," "technical data," "public domain," and "export." Defendants dispute each of these contentions.

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

12Plaintiff also argues that the ITAR is impermissibly vague in that the definitions of "defense articles," "defense services," and "technical data" all encompass the others. Specifically, a defense article "means any item *or technical data* designated in § 121.1 of this subchapter." 22 C.F.R. § 120.6 (emphasis added). Technical data, as defined in the ITAR and by the court in *Edler,* is information required for the manufacture or operation of defense articles or information directly relating to defense articles. 22 C.F.R. § 120.10. The definition of defense services distinguishes between defense articles and technical data. 2 C.F.R. § 120.9. Defendants argue that technical data is defined separately in the ITAR and in a manner that distinguishes it from actual commodities treated as defense articles such that it is not a defense article itself. However, the exact language of the ITAR does not comport with defendants' characterization of it. The definition of defense articles *includes* technical data, which according to its own definition can only be understood *in relation to*defense articles. To say this is vague would be generous, but it need not be voided for it is easily cured. The phrase "or technical data" as well as the third sentence of the definition referring to technical data must be removed from the definition of defense article. Accordingly, items listed on

the USML are defense articles and information relating directly to them are technical data. Read in this way, the three terms are not impermissibly vague.

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

14However, the same cannot be said of section 120.11(a)(8), which contains the exemption for information available to the public "through fundamental research in science and engineering". 22 C.F.R. § 120.11(a)(8). This subsection, like the academic exemption which exempts "general scientific, mathematical or engineering principles" commonly taught in schools and universities, 22 C.F.R. § 120.10(a)(5), does not give people, particularly those of arguably extraordinary intelligence who are themselves engaged in the ***1294**applied sciences, "a reasonable opportunity to know what is prohibited". *Grayned*, 408 U.S. at 108, 92 S.Ct. at 2298–99. Given the direct application of these exemptions to First Amendment protections, the uncertainty created in scientists about what speech is subject to regulation under the ITAR is unacceptable.

For example, fundamental research is defined as "basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community". 22 C.F.R. § 120.11(a)(8). As defendants themselves repeatedly attest, cryptographic algorithms and theory are often published in scientific journals. Crowell Decl., Exhs. 1–10; Joint Statement of Undisputed Facts ¶ 9. However, cryptographic algorithms are also covered by Category XIII(b) of the USML. Given these two facts, it would be hard for scientists to discern when their work was a defense article and when it was wholly exempt from the ITAR without going through a CJ determination before any effort at publication. In fields of applied science, what is commonly taught in universities may well overlap with what the government might choose to regulate. In this instance the deterrent effect on protected expression appears both real and substantial. *Young v. American Mini Theatres, Inc.*, 427 U.S. at 60, 96 S.Ct. at 2447. These academic exemptions from the definition of technical data, 22 C.F.R. §§ 120.10(a)(5) & 120.11(a)(8), are accordingly void for vagueness.

15Lastly, plaintiff challenges the term “export” as vague for two reasons. First, because it encompasses publishing and second, because what constitutes an export depends on whether an item is defined as a defense article or as technical data and those definitions are themselves vague. The first issue is more properly one of overbreadth and will be addressed below. The second is clarified by the modifications made by the court to the definition of defense article.

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

B. *Overbreadth*

16In a facial challenge to a law on grounds of overbreadth, a court must first “determine whether the enactment reaches a substantial amount of constitutionally protected conduct. If it does not, then the overbreadth challenge must fail.” *Village of Hoffman Est. v. Flipside, Hoffman Est.*, 455 U.S. 489, 494, 102 S.Ct. 1186, 1191, 71 L.Ed.2d 362 (1982).

Facial overbreadth is concededly “strong medicine” employed as a last resort when a limiting construction cannot be applied to a statute.*Broadrick v. Oklahoma*, 413 U.S. 601, 613, 93 S.Ct. 2908, 2916–17, 37 L.Ed.2d 830 (1973). In *Members of the City Council of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789, 104 S.Ct. 2118, 80 L.Ed.2d 772 (1984), the Court noted that “where the statute unquestionably attaches sanctions to protected conduct, the likelihood that the statute will deter that conduct is ordinarily sufficiently great to justify an overbreadth attack.” *Id.* at 801 n. 19, 104 S.Ct. at 2126 n. 19 (citing *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 95 S.Ct. 2268, 45 L.Ed.2d 125 (1975)). However, the Court also clarified the application of substantial facial overbreadth, saying there must be a “realistic ***1295** danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the Court....” *Id.* at 801, 104 S.Ct. at 2126. Merely being able to conceive of “some impermissible applications of a statute” is insufficient. *Id.* at 800, 104 S.Ct. at 2126.

Defendants argue that although the traditional rules of standing are modified in the context of an overbreadth challenge on First Amendment grounds, *Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491,

503, 105 S.Ct. 2794, 2801–02, 86 L.Ed.2d 394 (1984) (noting cases holding that one whose own speech is validly prohibited by statute may still challenge statute facially because it threatens others not before the court), that is not the case where the party before the court seeks to engage in protected speech that the statute purports to punish. In that case, there is "no want of a proper party to challenge the statute, no concern that an attack on the statute will be unduly delayed or protected speech discouraged." *Brockett*, 472 U.S. at 504, 105 S.Ct. at 2802. Accordingly defendants assert that because plaintiff cannot show a significant difference between his claims and those of third parties, the court must consider the overbreadth challenge as applied to plaintiff. Plaintiff disputes this by citing cases emphasizing that if a statute's overbreadth is substantial and its chilling effect significant, the entire statute may be invalidated to protect the First Amendment. *Lind v. Grimmer*, 30 F.3d 1115, 1122 (9th Cir.1994), *cert. den sub nom. Wang v. Lind*, 513 U.S. 1111, 115 S.Ct. 902, 130 L.Ed.2d 786 (1995) (distinguishing cases in which the only unconstitutional application was the one directed at the party before the court and where the chilling effect could be obviated by partial invalidation); *see also Board of Airport Comm'rs of Los Angeles v. Jews for Jesus, Inc.*, 482 U.S. 569, 573–74, 107 S.Ct. 2568, 2571–72, 96 L.Ed.2d 500 (1987).

17The court need not resolve this dispute over standing because the issues left unresolved are few, and for those that remain the nature of the challenge will not make a difference. The First Amendment does not "render inapplicable the rule that a federal court should not extend its invalidation of a statute further than is necessary to dispose of the case before it." *Brockett*, 472 U.S. at 502, 105 S.Ct. at 2801 (citation omitted). The court is mindful of that admonition. It has ruled on Category XIII(b) and technical data generally under prior restraint analysis; it has offered a curing instruction for the definition of "defense articles" and has invalidated the academic exemptions to technical data on vagueness grounds. All that remains are plaintiff's claims that the definition of export is overbroad and that the entire ITAR scheme is overbroad in that it assumes that all foreigners are terrorists. The latter strikes the court as patently absurd. The former can be disposed of quickly.

As noted above, "export" is defined with respect to defense articles as "[s]ending or taking a defense article out of the United States in any manner", 22 C.F.R. § 120.17(a)(1). With respect to technical data it means "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad". 22 C.F.R. § 120.17(a)(4). The provision governing the exportation of defense articles is clearly aimed mainly at conduct—at shipping tanks, missiles and the like abroad. Yet in regulating cryptographic software it also sweeps in speech. While the overbreadth of the provision in this respect is real, the court cannot say that it is "substantial as well, judged in relation to the statute's plainly legitimate sweep." *Broadrick*, 413 U.S. at 615, 93 S.Ct. at 2918.With respect to the export of technical data, this court is again bound by *Edler* regardless of whether it agrees with that disposition. There the Ninth Circuit added a

scienter requirement to the prohibition against exporting technical data in order to cure the overbreadth problem. *Edler,* 579 F.2d at 521.

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

III. *Administrative Procedures Act*

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

***1296** IV. *Preliminary Injunction*

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

Defendants assert that a preliminary injunction is unwarranted because teaching a class on cryptography does not violate the regulations. They also argue that the motion for a preliminary injunction is merely an attempt by plaintiff to circumvent export controls by distributing cryptographic software abroad in the name of academic freedom.

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

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

CONCLUSION

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

IT IS SO ORDERED.