CINDY A. COHN, ESQ.; SBN 145997
McGLASHAN & SARRAIL
Professional Corporation
177 Bovet Road, Sixth Floor
San Mateo, CA 94402
Tel: (415) 341-2585
Fax: (415) 341-1395

LEE TIEN, ESQ.; SBN 148216
1452 Curtis Street
Berkeley, CA 94702
Tel: (510) 525-0817

M. EDWARD ROSS, ESQ.; SBN 173048
STEEFEL, LEVITT & WEISS
A Professional Corporation
One Embarcadero Center, 30th Floor
San Francisco, CA 94111
Tel: (415) 788-0900

JAMES WHEATON, ESQ.; SBN 115230
ELIZABETH PRITZKER, ESQ.; SBN 146267
FIRST AMENDMENT PROJECT
1736 Franklin, 8th Floor
Oakland, CA 94612
Tel: (510) 208-7744

Attorneys for Plaintiff
Daniel J. Bernstein

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN)
) C 95-00582 MHP
Plaintiff,)
) PLAINTIFF'S MEMORANDUM OF
v.) POINTS AND AUTHORITIES IN) SUPPORT OF MOTION FOR PARTIAL UNITED STATES DEPARTMENT OF) SUMMARY JUDGMENT AND/OR
STATE et al.,) SUMMARY ADJUDICATION OF) ISSUES
Defendants.) F.R.C.P. 56
)
) Date: September 20, 1996
) Time: 12:00 p.m.) Judge: Hon. Marilyn Hall Patel
)

INTRODUCTION

When, if ever, may the U.S. Government require a private citizen to submit his ideas to a government agency for review and licensing prior to publication or public discussion? When, if ever, may the Government use such a process to censor publication of ideas about an entire subject area, namely the science of

cryptography?

Plaintiff PROFESSOR DANIEL BERNSTEIN ("PROF. BERNSTEIN") wishes to publish his own ideas about the science of cryptography in print, in the classroom and on the Internet. He seeks to engage in the free exchange of scientific ideas protected by both the freedom of speech and by academic freedom, "a special concern of the First Amendment." Keyishian v. Bd. of Regents, 385 U.S. 589, 603 (1967). The undisputed effect of the Arms Export Control Act, 22 U.S.C. §2778 et. seq. ("AECA") and its implementing regulations, the International Traffic in Arms Regulations ("ITAR") (hereinafter collectively referred to as the "ITAR Scheme"), is to require PROF. BERNSTEIN and others to submit their ideas about cryptography to the government for review, to register as arms dealers, and to apply for and obtain from the government a license to publish their ideas. Failure to do so results in severe civil and criminal penalties. In short, when ones ideas fall under the ITAR, instead of "publish or perish," the ITAR provides "publish and perish."

In the first phase of this litigation, the Government argued that since Plaintiff's ideas were expressed, in part, in source code, they were not protected by the First Amendment. This Court rejected that argument and held that source code is speech for purposes of the First Amendment. Opinion on Motion to Dismiss, April 15, 1996 at 20:20-22. (hereinafter "Opinion"). But the ITAR Scheme controls more than just source code; its definition of software extends into algorithms and design structures, the very building blocks of mathematics and computer science. In addition, the Ninth Circuit recognized nearly 20 years ago that the ITAR Scheme also controls much protected speech through its control of "technical data." United States v. Edler Industries, Inc., 579 F.2d 516, 520 (9th Cir. 1978). Accordingly, since it censors speech about cryptography both as software and as technical data, the ITAR Scheme must pass several stringent First Amendment tests.

This Motion first seeks summary adjudication that the ITAR Scheme, to the extent it controls speech about cryptography, must meet stringent First Amendment scrutiny. Plaintiff argues first, that as to the prior restraints, the ITAR Scheme must pass the test provided in New York Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart J., with whom White, J. joins, concurring)(hereinafter "Pentagon Papers"). Second, as to application of the ITAR Scheme as subsequent punishment for speech about cryptography, Plaintiff submits that the strict scrutiny tests apply. *E.g.* Austin v. Michigan Chamber of Commerce 494 U.S. 652, 654-655 (1990). This Motion also seeks partial summary judgment that there is no genuine issue of material fact that the ITAR Scheme, to the extent it controls speech about cryptography, fails three other standards of First Amendment jurisprudence: it lacks the procedural safeguards required by Freedman v. Maryland, 380 U.S. 51 (1965); it is vague; and it is overbroad. The common principle which runs through these three doctrines, and which the ITAR violates, is the requirement that grants of administrative discretion be limited by clear standards and that judicial review be available. With no limitations on administrative action, the ITAR Scheme "readily lends itself to harsh and discriminatory enforcement," Thornhill v. Alabama, 310 U.S. 88, 97 (1940) and "creates a threat of censorship that by its very existence chills free speech." Sec'y of State of Maryland v. Joseph H. Munson Co., 467 U.S. 947, 964 n. 12 (1984). Quite simply, the ITAR Scheme allows its administrative agencies to make inconsistent, incorrect and sometimes incomprehensible decisions censoring speech, all without the protections of judicial review or oversight.

STATEMENT OF FACTS

At the time of filing, Plaintiff was a Ph.D. candidate in mathematics at the University of California at Berkeley. He has since received his degree. He now teaches in the Department of Mathematics, Statistics and Computer Science at the University of Illinois at Chicago. PROF. BERNSTEIN has conducted research in the field of cryptography, the art and science of keeping messages secure. His work was developed on his own, without government funds or support, and is not classified. He intends to present his ideas, in all their forms, to the worldwide academic and scientific community. Despite this undisputed scientific, nonmilitary intention, Defendants have told Plaintiff that he cannot present his ideas.

PROF. BERNSTEIN's work in cryptography included developing an algorithm called Snuffle for scrambling and descrambling communications. He wrote one description of the Snuffle algorithm in English using mathematical formulas (hereinafter "Paper"). In order to express it as precisely as possible, he also wrote a description of the algorithm in a computer language. He called the final versions of these computer language descriptions Snuffle.c and Unsnuffle.c. (Collectively referred to hereinafter as "Snuffle 5.0"). Bernstein Decl. ¶¶6-7. Professors Abelson and Sussman of the Massachusetts Institute of Technology, have explained why algorithms are often written in programming languages :

Just as everyday thoughts are expressed in natural language, and formal deductions are expressed in

mathematical language, methodological thoughts are expressed in programming languages. A programming language is a medium for communicating methods, not just a means for getting a computer to perform operations---programs are written for people to read as much as they are written for machines to execute.

Abelson and Sussman, *Structure and Interpretation of Computer Programs*, preface, page xv. (1985). *See also* Declaration of Harold Abelson, ¶ 3-17. This view is also shared by the author of the "Bible" of computer programming, Professor Donald E. Knuth of Stanford University, who has written:

At first I thought programming was primarily analogous to musical composition -- to the creation of intricate patterns, which are meant to be performed. But lately I have come to realize that a far better analogy is available: **Programming is best regarded as the process of creating works of literature**, which are meant to be read.

Literature of the program genre is performable by machines, but that it not its main purpose. Computer programs that are truly beautiful, useful, and profitable must be readable by people. So we ought to address them to people, not to machines.

Knuth, *Literate Programming*, IX (emphasis in original). *See* Declaration of Carl M. Ellison ¶ 12. This view of computer programming languages as languages which fundamentally communicate between humans is widely recognized. For this reason, computer programs have been published in scientific journals for peer readership for over 25 years. Ellison Decl. ¶¶15-23.

PROF. BERNSTEIN wants to publish his cryptographic ideas as part of the normal process of academic, scientific and political exchange of ideas and information. This process lies at the heart of First Amendment as well as the scientific method, which requires that new ideas be continually tested and discussed in the "marketplace of ideas." Bernstein Decl. ¶¶46, 52; Appel Decl. ¶¶ 3-5, 17. Because the ideas developed in many areas of science involve computer code, the scientific method includes publication of such code. Today, moreover, scientific publication includes Internet publication. PROF. BERNSTEIN also wishes to publish his ideas in "sci.crypt," an Internet discussion group about cryptography. The Internet has become a significant place to publish all types of academic and scientific ideas. Publishing computer code on the Internet enables not only the evaluation of ideas, but also their incremental improvement.

Moreover, Plaintiff will teach a course on cryptography next year. Bernstein Decl. ¶¶53-63. Whether in class, during office hours, or on the Internet, he must be free to discuss cryptography with his students without a license. University classes in computer-related fields often have course syllabi, assignments, and materials available on the Internet; some require students to publish on the Internet. Miller Decl. ¶¶4-6. In addition, Plaintiff must be free to test out his ideas on colleagues before he finally decides to publish them.

STATUTORY AND REGULATORY FRAMEWORK

Section 38 of the AECA authorizes executive control of commercial "export" of "defense articles and defense services" through the power to designate "items" on the U.S. Munitions List ("USML") and to promulgate the ITAR. 22 U.S.C. § 2778(a)(1). The ITAR Scheme makes it unlawful "[t]o export or attempt to export from the United States any defense article or technical data or to furnish any defense service for which a license or written approval is required by this subchapter without first obtaining the required license or written approval" from the State Department ("State"). 22 C.F.R. § 127.1(a)(1); *see* 22 U.S.C. § 2778(b)(2). This basic premise is fairly straightforward. From this point, however, sorting out the various ITAR definitions and State interpretations of the text becomes difficult, if not impossible.

A. Key Definitions in the ITAR Scheme As It Relates to Plaintiff's Claims

The ITAR Scheme definitions which are most important to Plaintiff's claims are those of "defense articles and defense services," "software," "technical data," and "export." It is through the interactions of these that protected expression is restrained and that the problems of excessive discretion, vagueness and overbreadth are most obviously manifest. For example, key definitions such as "defense article," "technical data" and "defense services" refer to each other in circular fashion. Yet these very labels determine what activities constitute "export."

1. Defense Articles and Defense Services

"'[D]efense articles and defense services' means, with respect to commercial exports subject to [22 U.S.C.

§2778], those items designated . . . pursuant to" the USML. 22 U.S.C. § 2794(7). The USML includes "software with the capability of maintaining secrecy or confidentiality of information or information systems." 22 C.F.R. §121.1 (XIII)(b)(1). Thus cryptographic software is apparently a defense article. Technical data is also included as a defense article. 22 C.F.R. §120.6; 123.1(b) and §123.1(e). Finally, defense services are defined as "furnishing assistance" or technical data to foreign persons. 22 C.F.R. §120.9(1) and (2).

2. Software

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). Thus, contrary to most reasonable expectations, software is not limited to computer code. It also includes system designs, algorithms and logic flows, the very building blocks of many mathematical concepts and scientific ideas, and by its own language "is not limited" to just those.

3. Technical Data

"Technical data" appears several places throughout the ITAR Scheme, creating confusing circularity. As mentioned above, the definition of defense articles includes technical data, thus making technical data on its face is a subset of defense articles. Furthermore, defense articles include "technical data recorded or stored in any physical form," so a book or diskette on which technical data is recorded is apparently a defense article. Technical data itself includes several different types of ideas and information. The relevant definitions of technical data are:

Information, other than software as defined in § 120.10(d) [sic], which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation. . . .

Software as defined in § 121.8(f) of this subchapter directly related to defense articles[.]

22 C.F.R. § 120.10(a)(1), (a)(4). Because software is defined as technical data, cryptographic software appears to be both a defense article and as technical data, and the "furnishing" of software is a defense service.

4. Export

The AECA does not define "export." In the ITAR, despite the overlap between defense articles and technical data noted above, the meaning of "export" for each differs significantly. "Export" of defense articles is defined as "sending or taking a 'defense article' out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data." "Export" of technical data includes disclosing orally or visually or transferring technical data to any foreign person, whether abroad or <u>in the United States</u>. 22 C.F.R. § 120.17(a)(1), (a)(4). (Emphasis added)

B. <u>How The ITAR Scheme Was Applied To PROFESSOR BERNSTEIN</u>

Vaguely aware of the Defendants' restrictions on cryptography, Plaintiff contacted State to learn whether he needed a license to publish his ideas. He was told to submit a Commodity Jurisdiction ("CJ") request per former provision 22 C.F.R. § 120.4, which he did. Bernstein Decl. ¶17. In response to this first CJ, Defendants stated that a license was required. Plaintiff then engaged in a protracted, frustrating and ultimately unsuccessful attempt to learn how the Defendants interpreted the ITAR Scheme. Bernstein Decl. ¶¶16-42. *See* Miller Decl. ¶¶ 14-45; Junger Decl. ¶¶ 8-16; Johnson Decl. ¶¶22-33; Zimmermann Decl. ¶¶17-24 and NRC Report at 4-14 to 4-18, 4-30 to 4-33 and 4-47.

Eventually Plaintiff submitted a second round of five separate CJ Requests, each of which asked if he could publish a different item directly related to Snuffle. Plaintiff sought to give the Defendants the opportunity to consider each item separately. Bernstein Decl. ¶¶34-36. Defendants informed Plaintiff that all of the items were "subject to the licensing jurisdiction of the Department of State." Bernstein Decl. ¶37.

Over two years later and after having been sued, Defendants issued a "clarification" letter directly rejecting the clear meaning of their previous responses. Defendants belatedly indicated that the source code items were defense articles, the Instructions "appeared to be" technical data and the Paper, over which they had first asserted control in 1992, "appeared" not to be controlled at all. Bernstein Declaration, ¶41.

C. Impact of the ITAR Scheme

The facial reach of Defendants' determinations is staggering. PROF. BERNSTEIN may not take or send Snuffle 5.0 source code outside of the U.S. in any manner. He may not present Snuffle 5.0 to a conference abroad or communicate it privately to an overseas colleague (even a U.S. citizen). *See also* Junger Decl. ¶¶ 18-23. He may not publish Snuffle 5.0 on the Internet in any form. *See also* Demberger Decl. ¶¶ 2-13 and Miller Decl.¶¶ 14-17, 20. Although the regulations are vague on this point, it appears that he may not even publish it in print, since published journals or books are inevitably sent abroad. *See also* Junger Decl. ¶¶ 23-28. In short, he is prevented from placing his source code into the "marketplace of ideas."

As to the Instructions, which Defendants have apparently belatedly designated as "technical data," the restraint is similarly broad. Disclosing technical data to a foreign person anywhere is "export," sweeping in face-to-face teaching of a foreign student, phone calls with foreign colleagues, presentations at conferences and electronic or print publication. *See also* Junger Decl. ¶¶ 18-28. In each instance, technical data would inevitably be disclosed to a foreign person. Even displaying technical data in this Court's public courtroom as part of this case is "export" if a foreign person is seated in the gallery.

Finally because the labels of defense article and technical data are not mutually exclusive, Snuffle 5.0 source code is facially subject to the "technical data" export provisions as well, while the Instructions are facially subject to the "defense article" export provisions, and any communication of either is a "defense service". In sum, regardless of whether scientific information is labeled as a "defense article," "technical data," or "defense service," the ITAR significantly restricts its communication.

ARGUMENT

I. THE ITAR SCHEME REGULATES SPEECH.

A. The Controlled Items Are Speech

Since this Court has held that source code is speech for First Amendment purposes, the Snuffle 5.0 source code at issue here is speech. There is no dispute that the Instructions, now evidently declared "technical data" by Defendants, are speech. Finally, the Snuffle Paper was recognized as speech by this Court. Opinion 14:17-23. Since this Motion attacks the facial overbreadth, vagueness and lack of procedural protections in the ITAR Scheme, each of these items is part of the "speech." Indeed, the fact that Defendants improperly applied these regulations to Paper, an obvious speech item, is a perfect example of why the ITAR is so constitutionally offensive.

B. On Its Face the ITAR Scheme Regulates Scientific Speech

Scientific speech is entitled to the highest degree of First Amendment protection. The ITAR Scheme seeks to license scientific expression in three ways. First, the technical data provision reaches scientific expression by including "information in the form of blueprints, drawings, photographs, plans, instructions and documentation" relating to defense articles. 22 C.F.R. § 120.10(a)(1). Second, the regulation of software includes speech since computer software in source code form is speech. Opinion at 20:20-22. Third, the ITAR Scheme seeks to control more than code in its definition of software, including "design", "logic flow" and "algorithms" as part of the definition and thus sweeping in the very building blocks of much mathematics and computer science.

Defendants have argued that they only seek to restrict ideas written in programming languages. While Plaintiff disputes this, even if it were true, speech is burdened. In conditioning publication of ideas upon their not being written in a programming language, Defendants seek to prescribe the form and content of expression. Expressing algorithms in a computer language increases precision of communication.

Each step of an algorithm must be precisely defined; the actions to be carried out must be rigorously and unambiguously specified for each case. The algorithms of this book will hopefully meet this criterion, but since they are specified in the English language, there is a possibility the reader might not understand exactly what the author intended. To get around this difficulty, formally defined 'programming languages' or 'computer languages' are designed for specifying algorithms, in which every statement has a very definite meaning. Many of the algorithms in this book will be given both in English and in a computer language.

D. Knuth, 1 *The Art of Computer Programming: Fundamental Algorithms* 5 (1968).

To write an algorithm as a computer program, therefore, is to make a choice among various ways of saying something. The Government has no authority to make that choice for private citizens. "[T]hat a speaker has the autonomy to choose the content of his own message" is "the fundamental rule of protection under the

First Amendment." Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston, 115 S.Ct. 2338, 2347 (1995).

C. On its Face and as Applied to PROF. BERNSTEIN, the ITAR Scheme Infringes Academic Freedom

Academic freedom "has long been viewed as a special concern of the First Amendment." Regents of the University of California v. Bakke, 438 U.S. 265, 312 (1978); Keyishian, 385 U.S. at 603. Academic freedom protects more than just what Prof. Bernstein wants to teach in the classroom; it protects his right to publish books and articles and to exchange the fruits of his work and research with others. *See* Gordon & Breach Science Publishers v. AIP, 859 F.Supp. 1521, 1541 (S.D.N.Y. 1994) ("debate . . . in academic journals" is "near the core of the First Amendment"). In Bakke, the Supreme Court noted:

It is the business of a university to provide that atmosphere which is most conducive to speculation, experiment and creation. It is an atmosphere in which there prevail the "four essential freedoms" of a university - to determine for itself on academic grounds who may teach, what may be taught, how it shall be taught, and who may be admitted to study.

Bakke, 438 U.S. at 312 *quoting* Sweezy, 354 U.S. at 263 (Frankfurter, J., concurring).

Scientific and technical exchange of information is also protected as part of academic freedom. "The classroom is peculiarly the 'marketplace of ideas.'" Keyishian, 385 U.S. at 603. "Teachers and students must always remain free to inquire, to study and to evaluate, to gain new maturity and understanding." Sweezy v. New Hampshire, 354 U.S. 234, 250 (1957)(quotation and citation omitted); *see* Rosenberger v. Univ. of Virginia, 115 S.Ct. 2510, 2520 (1995) (university setting "at the center of our intellectual and philosophic tradition").

In a 1981 memorandum, the Justice Department Office of Legal Counsel ("OLC") warned that the ITAR scheme's coverage "is so broad that the revised provisions could be applied to persons who are not directly connected or concerned in any way with any foreign conduct carrying dangerous potential for the United States . . . [such as] to communications of unclassified information by a technical lecturer at a university." Tien Decl., Exhibit A, OLC memo for Robinson at 212 (Bates stamp page 60057); *see also* Bates stamp pages 60007-8 and 600017-18. That scenario is before this Court. Prof. Bernstein's work is neither classified nor directly connected with any such foreign conduct, yet it is restricted by the ITAR Scheme.

The ITAR Scheme violates all four freedoms raised in Bakke. "The heart of the system consists in the right of the individual faculty member to teach, carry on research, and publish without interference from the government." Dow Chemical Co. v. Allen, 672 F.2d 1262, 1275 (7th Cir. 1982) (quotation and citation omitted). Prof. Bernstein is not free to teach cryptography by teaching about the development and analysis of cryptographic computer programs; he needs Defendants' approval and a government license which he cannot practically obtain and which is revocable at whim.

D. Foreign Persons Have First Amendment Rights to Speak and Receive Information Which Are Abridged by the ITAR Scheme's Discrimination Against Them

The ITAR Scheme violates two more of Bakke's "four essential freedoms" by restricting who may teach and who may be admitted to study. By doing so, it reaches overbroadly into the speech rights of foreign persons. *See* American-Arab Anti-Discrimination Committee, et al v. Reno, 70 F.3d 1045, 1063 (9th Cir. 1995). Under the ITAR Scheme, no foreign person, not even a foreign Nobel prize winner teaching at Stanford, may obtain an export license. 22 U.S.C. §2778(g). Moreover, because a U.S. speaker "exports" by disclosing technical data to a "foreign person," foreign persons' First Amendment rights to receive information are restricted. As a result, PROF. BERNSTEIN might have to exclude foreign students from his cryptography course in order to engage in the open exchange of cryptography ideas in the classroom. Yet the Supreme Court long ago held that "where a [willing] speaker exists . . . the protection afforded is to the communication and to its source and recipients both." Virginia Pharmacy Bd. v. Virginia Consumer Council, 425 U.S. 748, 756 (1976) (rights of consumers to receive price advertising); *See* United States v. National Treasury Employees Union, 115 S.Ct. 1003, 1015 (1995). ("NTEU")

E. By Restricting the Ability of People to Protect the Privacy of Their Communications, the ITAR Scheme Chills Speech

Freedom to speak would mean little if one could not control who could overhear the speech. Thus, the First Amendment includes the right to speak confidentially. *See* United States v. United States District Court, 407

U.S. 297, 314 (1972). It prevents compelled speech. Hurley v. Irish-American Gay Group of Boston, 115 S.Ct. 2338 (1995). It protects anonymous speech. McIntyre v. Ohio Elections Com'n, 115 S.Ct. 1511, 1516 (1995). It prevents compelled disclosure of those with whom one associates and speaks. NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958). It extends to a person's right to communicate with foreigners. Bullfrog
Films, Inc. v. Wick, 842 F.2d 502, 509, n.9 (9th Cir. 1988) (remanded on other grounds, 959 F.2d. 778 (9th Cir. 1992)).
For electronic speech, encryption is like an "envelope" which may only be opened by authorized recipients. There can be little doubt that a statute or regulation requiring persons using the U.S. mails to write on postcards or restricting the availability of envelopes to licensed individuals would significantly affect the content of mailed expression. Without envelopes, people would only express facts or ideas that they were willing to let anyone read. Thus, cryptography, like paper and ink, is inherently imbued with First Amendment significance. *Cf.* Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 575, 585 (1983) (invalidating "use tax" on paper and ink products consumed in newspaper publication).

II. THE ITAR SCHEME IS A PRIOR RESTRAINT WHICH FAILS THE HEAVY PRESUMPTION AGAINST CONSTITUTIONAL VALIDITY THAT THE FIRST AMENDMENT DEMANDS

Any scheme that requires a permit or license for speech which may be granted or withheld in the discretion of an official makes the exercise of First Amendment freedoms contingent upon the uncontrolled will of an official and is a . . . prior restraint upon the enjoyment of such freedoms. Staub v. Baxley, 355 U.S. 313, 322 (1958). Those schemes represent "the most serious and least tolerable infringement on First Amendment rights." (Nebraska Press Ass'n v. Stuart, 427 U.S. at 539, 559 (1976). As a result, any system of prior restraint of expression comes bearing a heavy presumption *against* its constitutional validity. Pentagon Papers, 403 U.S. at 714 (quotation and citations omitted)(emphasis added). This heavy presumption cannot be overturned and publication cannot be prevented -- even as to matters involving military affairs -- unless it is shown that publication will "surely result in direct, immediate, and irreparable damage to our Nation or its people." Id., at 730 (Stewart, J. concurring). In addition, licensing schemes requiring prior government approval of communication are facially void if impermissibly vague or excessive in reach. Lovell v. City of Griffin, 303 U.S. 444, 452-53 (1938).
The ITAR, which requires a license prior to publication, is just such a prior restraint. It fails to overcome the "unusually heavy presumption against constitutional validity" required by the First Amendment.

A. THE SCHEME CONTAINS AT LEAST FOUR PRIOR RESTRAINTS

1. The CJ Process is a Prior Restraint

As noted above, figuring out what one can and cannot do under ITAR involves entering a circular maze of definitions. *See supra* at pages 5-8. Because the reach of the ITAR scheme is so unclear, its requirements so onerous, and liability both criminal and civil so severe, individuals have a powerful incentive to invoke the CJ procedure if there is even the slightest possibility that the Government could later determine that their work is, or is "directly related to" an item on the USML. *See* Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations, 413 U.S. 376, 390 (1973) (a "special vice" of prior restraint is "inducing excessive caution in the speaker"). PROF. BERNSTEIN, like many others, was unsure about the reach of the ITAR Scheme. When he asked Defendants whether he could publish his ideas, PROF. BERNSTEIN was advised to use the Commodity Jurisdiction process. Later, when he submitted his items, he was advised that a license was required. However, even if PROF. BERNSTEIN had learned that no license was needed, he would still have experienced significant pre-publication delay. Thus the CJ process itself is a prior restraint, whether or not something is ultimately deemed controlled, because it delays publication. Freedman, *supra*, 380 U.S. at 57 (delay is a form of unbridled discretion).

2. The Registration and Fee System Is a Prior Restraint.

When Defendants determined that he must seek a license, PROF. BERNSTEIN was first required to register as an arms exporter. Registration amounts to a license to seek a license; one may not apply for a license without first registering (22 C.F.R. §§122.1(c), 120.4(b)) and paying fees. 22 C.F.R. §§ 122.2(a), 122.3(a). This payment requirement alone creates a prior restraint. *See* Forsyth County v. Nationalist Movement, 505 U.S. 123, 130 (1992). At best, registration adds even more delay; at worst, Defendants have unreviewable discretion in deciding whether to accept registration (*see* discussion, *infra*, at 18).

Also, registration is expressly "a means to provide the U.S. Government with necessary information about who is involved in certain manufacturing and exporting activities." 22 C.F.R.§ 122.1(c). This requirement makes no sense for Plaintiff, a math professor, and acts as a prior restraint by infringing upon his right to publish his ideas without telling the government about it. *See* McIntyre 115 S.Ct. at 1516.

3. The Licensing Decision Is a Prior Restraint.

Plaintiff did not apply for a license to publish. An application would have been futile. An export license application for defense articles must designate the "country of ultimate destination;" the exporter "must ascertain the specific end-user and end-use prior to submitting an application," 22 C.F.R. § 123.9(a); *See also* id. at § 123.21(a). This cannot be done when one publishes source code in a book, journal or online discussion group, since one does not know who will receive it. As a practical matter, then, it is impossible to comply with the licensing requirement when one wishes to publish.

Equally important, no standards control Defendants' licensing decision. "[A]ny application for an export license or other approval under this subchapter may be disapproved . . . whenever" the State Department "deems such action to be in the furtherance of world peace, the national security or the foreign policy of the United States, or is otherwise advisable." 22 C.F.R. §126.7(a)(1). Thus, CJ and export license determinations are prior restraints under Staub (355 U.S. at 322), as they are completely discretionary.

4. The ITAR's Reporting/Recordkeeping Mandate Is a Prior Restraint.

Even when an export license is granted, the ITAR impose numerous requirements which cannot practically be met when the speaker wishes to publish. In other cases, the export need not be licensed, but the regulations nonetheless burden communication.

For example, shipments of defense articles generally require a Shipper's Export Declaration. 22 C.F.R. § 123.16(a) ("SED"). If Plaintiff wishes to mail a copy of Snuffle 5.0 or the Instructions to an overseas colleague, he must show when and how the export took place. 22 C.F.R. § 123.22(e). The SED must be authenticated by either the postmaster or Plaintiff, and he must return the SED to State when the mailings are completed. 22 C.F.R. § 123.24. Also, State has the discretion to require that a nontransfer and use certificate be filed in any export. This certificate must be executed by the foreign consignee and foreign end-user, prior to issuance of a license and license applicant. State may also, in its discretion, require that the "appropriate authority" of the foreign end-users own government sign the certificate before a license is issued. 22 C.F.R. § 123.10(c).

Even if a license is granted, the ITAR's recordkeeping requirements present another prior restraint. Exporters must maintain records about their activities for five years after expiration of a license. 22 C.F.R.§ 122.5(a). This recordkeeping requirement includes not only exports but the "disposition" of defense articles. Thus, PROF. BERNSTEIN must keep logs of his academic work and specify with whom any developments or refinements were discussed. Obviously it is a severe burden to comply with such onerous requirements in the context of academic publication.

B. THE ITAR SCHEME MUST MEET PENTAGON PAPERS' MANDATE OF EXACTING SCRUTINY

The "chief purpose" of the First Amendment is "to prevent previous restraints upon publication." Near v. Minnesota ex rel. Olson, 283 U.S. 697, 713 (1931). Because the ITAR Scheme as extended to speech about cryptography is just such a previous restraint upon publication, it must pass exacting scrutiny to be upheld. *See* CBS, Inc. v. U.S. District Court, 729 F.2d 1174, 1178 (9th Cir. 1983) (standard by which prior restraints on speech are reviewed is an "extraordinarily exacting" one). Thus, Defendants must prove that in every communication restrained by the ITAR, including PROF. BERNSTEIN's speech: (1) there exists a real, articulable likelihood of "direct, immediate, and irreparable damage" (Pentagon Papers at 730)(Stewart J. concurring) and (2)) the regulation at issue is necessary to prevent the injury so established. Burson v. Freeman, 504 U.S. 191, 199 (1992). Unless both mandates are satisfied, the ITAR Scheme cannot be applied to speech about cryptography.

1. Defendants Must Show That "Direct, Immediate And Irreparable Damage Will Surely Result" If Publication Is Not Restrained.

The First Amendment's heavy presumption against the validity of prior restraints requires that Defendants

offer more than averments that publication may result in an alleged harm. The Government must instead come forward with credible, factual *evidence* that publication of academic and scientific speech about cryptography, including source code, will surely result in direct, immediate, and irreparable damage to our Nation or its people. Pentagon Papers at 730 (Stewart, J. concurring). *See* Turner Broadcasting Systems, Inc. v. FCC, 114 S.Ct.2445, 2470 (1994) ("When the Government defends a regulation on speech as a means to. . .prevent anticipated harms, it must do more than simply 'posit the existence of the disease sought to be cured.' . . .It must demonstrate that the recited harms are real, not merely conjectural."). This high standard is applied despite the recognized fact that:

Much speech is dangerous. Chemists whose work might help someone build a bomb, political theorists whose papers might start political movements that lead to riots, speakers whose ideas attract violent protesters, all these and more leave loss in their wake.

American Booksellers Ass'n, Inc. v. Hudnut, 771 F.2d 323, 333 (7th Cir. 1985), *aff'd mem*., 475 U.S. 1001, *reh'g denied*, 475 U.S. 1132 (1986). In cases involving claims of national security, the Supreme Court long ago explained the nature of speech which might be properly restricted under this test as including "the sailing dates of transports or the number and location of troops" during wartime. Near, 283 U.S. at 716.

In Pentagon Papers a former Pentagon employee, Dr. Daniel Ellsberg gave to the media secret, classified government reports called the Pentagon Papers. The Papers recorded U.S. involvement in the Vietnam War and, in June 1971, the *New York Times* decided to publish them. The Government sought to enjoin publication, asserting that the release of that information would harm U.S. foreign intelligence gathering by:

[m]inimiz[ing] our chance of successful interception. Cutting down successful interception by our communication intelligence will directly affect our military operations. Signal intelligence now gives direct support to our troops today, and saves many lives.

Sims, *Triangulating the Boundaries of the Pentagon Papers*, 2 Wm. & Mary Bill of Rights J. 341, 449 (1993) (reprinting declassified portions of the government's brief in Pentagon Papers).

However, while acknowledging that release of some information in the reports may harm national security concerns, the Court, on expedited review, declined the requested injunction, concluding that the Government had failed to establish a direct link between publication and a resulting immediate and irreparable injury to the U.S. or its citizenry:

. . . I cannot say that disclosure of any of [the documents at issue] will surely result in direct, immediate, and irreparable damage to our Nation or its people. That being so, there can under the First Amendment be but one judicial resolution of the issues before us. I join the judgments of the Court.

Pentagon Papers at 730 (Stewart, J. concurring).

Here, too, Defendants have asserted that the government interest in the control of speech about cryptography by the ITAR is "the need to control the availability of cryptography from the United States so that foreign intelligence gathering functions are not harmed." Def. Memorandum In Support of Motion to Dismiss, at 13. There is, as yet, nothing in the record to establish a direct and immediate link between publication of academic and scientific speech relating to cryptography and irreparable damage to U.S. intelligence gathering. However, to survive exacting scrutiny, Defendants must also show that such efforts will surely result in direct, immediate and irreparable injury to our Nation or its people.

Indeed, the Government arguably faces an even greater burden here, because it is not restraining specified and classified materials directly concerning an ongoing war, as the case in Pentagon Papers. Here the Government claims the general power to license or censor information on certain scientific subjects, including protected domestic academic activity and publication. Further, it claims this power when the nation is not at war. Keeping in mind the Supreme Court's admonition that "[T]he validity of a restraint on speech in each case depends on careful analysis of the particular circumstances," Speiser v. Randall, 357 U.S. 513, 521 (1958), this Court must determine whether the Government's justifications here are sufficient to justify a scheme with such widespread peacetime impact. *See* NTEU, 115 S.Ct. at 1014 (1995) ("widespread impact...gives rise to far more serious concerns than could any single [ ] [decision and] chills potential speech before it happens.")

2. The ITAR Must Be Narrowly Drawn And Alleviate The Alleged Harm.

Even if Defendants are able to satisfy Pentagon Papers' causation and "direct, immediate and irreparable damages" mandates, they must further "demonstrate. . .that the [ITAR scheme] will in fact alleviate these harms in a direct and material way" (Turner, 114 S.Ct. at 2450), and that the harm alleged "cannot be militated by less intrusive measures." CBS, Inc. v. Davis, 114 S.Ct. at 914 (Blackmun, J., in chambers).

III. THE ITAR SCHEME IS ALSO A CONTENT-BASED SPEECH RESTRICTION WHICH MUST SURVIVE THE STRICT SCRUTINY THAT THE FIRST AMENDMENT DEMANDS

Even if the requirements of Pentagon Papers are met, the subsequent punishment provisions of the ITAR, which also impact speech about cryptography, must pass constitutional scrutiny. Determining whether a governmental regulation of speech is permissible under the First Amendment depends, in part, on whether the restriction is content-based or content-neutral. A content-based restriction is subjected to strict scrutiny and is constitutional only if the government shows the "regulation is necessary to serve a compelling state interest and that it is narrowly drawn to achieve that end." Perry Educ. Ass'n. v. Perry Local Educators' Ass'n., 460 U.S. 37, 45 (1983). *See* Burson v. Freeman, 504 U.S. at 197-198; Simon & Schuster, Inc. v. N.Y. Crime Victims Bd., 502 U.S. 105, 116-118 (1991).

As explained below, the ITAR Scheme as it is applied to cryptography is the very definition of a content-based speech restriction. It must, therefore, withstand strict scrutiny to survive.

A. THE ITAR SCHEME IS CONTENT-BASED

1. The ITAR Scheme is Content-Discriminatory On Its Face

A restriction against speech may be content-based either because it favors or disfavors certain viewpoints, or because it discriminates among various subjects. Consolidated Edison Co. v. Public Service Comm'n., 447 U.S. 530, 537 (1980). *See* Burson v. Freeman, 504 U.S. at 197. On its face, the ITAR Scheme restrictions on cryptography treat both software and academic and scientific speech differently based on their content in at least three key respects.

First, the ITAR Scheme is a content-based regulation because, at its most fundamental level, the scheme restricts academic and scientific discussion of the entire topic of cryptography. *See* Consolidated Edison, *supra*, 447 U.S. at 537. Whether defined as a defense article or technical data, cryptographic software, together with its essential academic and scientific building blocks (*e.g.*, source code, algorithms, and logic flows), and instructions as to its use, are all swept within the ITAR Scheme's prohibition. As a result, as explained on pages 9-10, *supra*, one may not discuss these items in any form on the Internet, at an international academic conference, privately with a foreign colleague, or on its face even in the more traditional printed format. The ITAR Scheme is content-based because it removes discussion on the entire topic of cryptography from the "marketplace of ideas." "[A]bove all else, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." Police Department of Chicago v. Mosley, 408 U.S. 92, 95 (1972). By picking and choosing *by subject matter* that which is allowed and that which is not, the ITAR scheme is antithetical to the First Amendment.

Second, as a related matter, the ITAR Scheme requires that Defendants to review software and academic and scientific information and appraise its possible uses, strength, and effectiveness, to determine whether or not it is subject to the ITAR Scheme. Such inquiries are inherently content-driven. In City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993), Cincinnati sought to defend, against a First Amendment challenge, an ordinance banning news-racks distributing commercial publications from public sidewalks, while permitting similar news-racks purveying newspapers. The Court concluded that by any commonsense understanding of the term, the ban in this case is 'content-based' because whether any particular newsrack falls within the ban is determined by the content of the publication resting inside that newsrack. Id., 507 U.S. at 429. The same is true here. Under the ITAR Scheme, Defendants must review the content of the various expressions to determine whether or not they are prohibited.

Finally, by prohibiting encryption software, the ITAR Scheme indirectly restricts a particular mode of expression -- private speech. Thus, in the same way as prohibiting whispering would force one to announce a

private declaration of love to the world, or preventing the use of envelopes would compel an attorney to communicate with her foreign client by postcard, the ITAR Scheme restricts the sending of electronic communications in a mode that limits who can read them. However, our nation's courts have consistently held that singling out particular modes of expression amounts to content-based discrimination under the First Amendment. *See* McIntyre 515 U.S. at 1516. (First Amendment extends to anonymous speech); Yniguez v. Arizonian for Official English, 69 F.3d 920, 934-936 (9th Cir. 1995) (en banc), *cert granted*, 64 U.S.L.W. 3639 (U.S. Mar. 25, 1996) (No.95-974) (communications in language other than English held a protectible "mode of expression" under the First Amendment).

2. The ITAR Scheme Contains the Facial Indications of Viewpoint Discrimination

As a related matter, the ITAR also contains facial indicia of viewpoint discrimination in at least two respects. First, defendants have singled out cryptography for differential treatment. 22 C.F.R. § 121.8(f). This is so despite the existence of considerable interest in, and continuing public debate and governmental policy-making on, the subject of cryptography. *See generally* NRC Report, attached as Exhibit E to Tien Decl. at Preface, vii-xiii. Thus, export controls are a tool by which the government controls public views about cryptography. *See* id., at 4-1. It has long been held, however, that "power in government to channel the expression of views is unacceptable under the First Amendment." Bellotti, 435 U.S., at 785 (footnote omitted). Viewpoint-based suppression presents a risk even more serious than content discrimination. R.A.V. v. City of St. Paul, 505 U.S. 377, 391 (1992) (prohibiting "fighting words" on disfavored topics "goes even beyond mere content discrimination, to actual viewpoint discrimination"). The government is not neutral in this policy debate; it champions one type of encryption, "key escrow." NRC Report at xi, *see generally* Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U.Pa.L.Rev. 709 (1995). As the Supreme Court noted in Bellotti, "[E]specially where . . . suppression of speech suggests an attempt to give one side of a debatable public question an advantage in expressing its views to the people, the First Amendment is plainly offended." Bellotti, 435 U.S. at 785-789 (footnote omitted).

Second, the ITAR permits dissemination of cryptography to the extent that discussion encompasses only "public domain" information and "information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities." 22 C.P.R. § 120.10(a)(5). At the same time, however, the ITAR Scheme restricts discussion on the same topic of new ideas, technological advances, original work, and minority views not "commonly taught in schools, colleges, and universities." As such, from a scientific standpoint the ITAR is analogous to a regulatory scheme permitting the once-commonly taught view that the sun revolved around the earth, while at the same time prohibiting publication of Copernicus' new and different ideas.

3. Defendants Cannot Recast The Content-Based ITAR As Content- Neutral Under The "Expressive Conduct" Doctrine of U.S. v. O'Brien

Defendants attempt to transmogrify the content-based ITAR into content-neutral regulation aimed at expressive "activity" or "conduct" requiring less rigid constitutional analysis under United States v. O'Brien, 391 U.S. 367 4(1968) (burning draft card for expressive reasons). The assertion is based on Defendants' argument that Plaintiff's cryptographic software, its underlying academic and scientific foundations (*e.g.*, source code, algorithms, and logic flows), and instructions as to its use, are functional "conduct," as opposed to pure speech. However O'Brien applies only when "[a]pplication of a facially neutral regulation . . . incidentally burdens speech." United States v. Albertini, 472 U.S. 675, 687 (1985). Plaintiff has already shown that the ITAR Scheme is not facially content neutral; that alone renders O'Brien inapplicable.

In addition, Defendants' argument has already been rejected by this Court:

Whether source code and object code are functional is immaterial to the analysis at this stage. Contrary to Defendants' suggestion, the functionality of a language does not make it any less like speech. . . . Thus, even if Snuffle source code, which is easily compiled into object code for the computer to read and easily used for encryption, is essentially functional, that does not remove it from the realm of speech. Instructions, do-it-yourself manuals, recipes, even technical information about hydrogen bomb construction, *see* United States v. Progressive, Inc., 467 F.Supp. 900 (W.D. Wisc. 1979), are often purely functional: they are also speech. Opinion, at pp.16-18.

Moreover, the ITAR Scheme directly burdens speech because it is directed at communication by licensing

"disclosure" by U.S. persons and forbidding "disclosure" by foreign persons. Defendants themselves have stated that the ITAR Scheme applies to "professional and academic presentation and informal discussions . . . constituting disclosure of cryptologic technical data to foreign nationals." Munitions Control Newsletter, attached at Tien Decl., Exhibit E, N.R.C. Report, Box 4.11, (discussed at 4-30 to 4-31). Even the OLC agrees on this point:

[E]ven a cursory reading of the technical data provisions reveals that those portions of the ITAR *are directed at communication*. A more stringent analysis than the O'Brien test is therefore mandated.

Opinion, at p. 31, n. 17 (citing Tien Decl. Exh. A, at 60084, n. 16) (emphasis added). In short, because the ITAR Scheme is not content neutral and is directed at speech and communication and not conduct, O'Brien is not the appropriate test under which to evaluate Plaintiff's claims.

B. THE ITAR SCHEME MUST PASS STRICT SCRUTINY

As a content-based restriction, the ITAR must be subjected to the "compelling state interest" and "narrowly tailored" tests which comprise strict scrutiny.

1. Defendants Must Show That The Application Of The ITAR Scheme To Speech About Cryptography Is Necessary To Further A Compelling State Interest.

To justify a restriction against speech under strict scrutiny, it is not enough that the government identify some interest falling within the sphere of legitimate government concern. Rather, the asserted interest must be a compelling one. "Mere legislative preferences or beliefs respecting matters of public convenience may well support regulation directed at other personal activities, but be insufficient to justify such as it diminishes the exercise of rights so vital to the maintenance of democratic institutions. Schneider v.New Jersey, 308 U.S. 147, 161 (1939), *quoted in* Schad v. Borough of Mt. Ephraim, 452 U.S. 61, 69 (1981). The Government must be prepared to articulate, and support, a reasoned and significant basis for its decision. Schad at 77 (Blackmun, J. concurring). Furthermore, in light of the "danger of censorship" presented by a facially content-based statute, Leathers v. Medlock, 499 U.S. 439, 448 (1991), the law may be constitutionally employed only when it is "*necessary* to serve the asserted [compelling] interest." Burson v. Freeman, 504 U.S. at 199 (emphasis added).

In Edler the Ninth Circuit explained the government interest in the ITAR Scheme: "controlling the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise." Edler 579 F.2d at 521. There is, as yet, no evidence in the record to support or even explain how this interest requires extending the reach of the ITAR Scheme to general academic and scientific publication on the subject of cryptography. *See infra* at pages 32-33. As the Supreme Court observed only weeks ago: " ...where, as here, the record before Congress or before an agency provides no convincing explanation, this Court has not been willing to stretch the limits of the plausible, to create hypothetical, non-obvious explanations in order to justify laws that impose significant restrictions upon speech." Denver Area Educational Telecommunications Consortium v. F.C.C. 1996 U.S. LEXIS 4261 *58-59.

2. The ITAR Must Be Narrowly Tailored

Even if Defendants were able to satisfy the compelling interest test, they further must show that the ITAR scheme is "narrowly tailored," i.e., that it is the least restrictive means of achieving its purposes. Boos v. Berry, 485 U.S. 312, 329 (1988). First, the law must actually advance the asserted interest, and the Court must determine for itself whether it does. *See* Eu v. San Francisco County Democratic Central Comm, 489 U.S. 214, 226-29 (1989); Bellotti, 435 U.S. at 789-90. Second, the law must not be overinclusive, it must not restrict a significant amount of speech that does not implicate the government interest. Simon & Schuster, 112 S.Ct. at 511. *See infra* at 37- 41. Third, there must be no less restrictive alternatives that would serve the interest approximately as well. Florida Star v. BJ.F., 491 U.S. 524, 538-40 (1989)(instead of banning class of statements, law might have to provide for case-by-case findings that statements indeed implicate government interest). Fourth, the law must not be underinclusive; it must not fail to restrict a significant amount of speech that harms the government interest about as much as the restricted speech does. *See* Florida Star, 491 U.S. at 540.

Again, Defendants have presented no evidence to support the assertion that the ITAR is the least restrictive means of achieving its stated purpose. What is apparent that this stage of the proceedings, however, is that the ITAR has adopted the most restrictive approach of prohibiting publication and public communication about

an entire subject area: the science of cryptography. "Broad prophylactic rules in the area of free expression are suspect. Precision of regulation must be the touchstone in an area so closely touching our most precious freedoms." NAACP v. Button, 371 U.S. 415, 438 (1963) (citations omitted).

IV. THE ITAR SCHEME DOES NOT CONTAIN THE PROTECTIONS REQUIRED BY FREEDMAN V. MARYLAND.

Regardless of the substantive scrutiny applied, in order to withstand Constitutional challenge the ITAR's regulation of speech must be procedurally sound. In Freedman, 380 U.S. at 51, the Supreme Court held that a system of prior restraints for screening obscene films was constitutional only if accompanied by procedural safeguards necessary "to obviate the dangers of a censorship system." Id., at 58. Thus, a scheme of prior restraints such as the ITAR's application to speech about cryptography is invalid unless "accomplished with procedural safeguards that reduce the danger of suppressing constitutionally protected speech." Southeastern Promotions v. Conrad, 420 U.S. 546, 559 (1975); Forsyth County, 505 U.S. at 131.

A. The AECA Statute Does Not Control Administrative Discretion.

Where a law authorizes a system of prior restraints, the statutory delegation must provide "narrowly drawn, reasonable and definite standards for the [administering] officials to follow." Niemotko v. Maryland, 340 U.S. 268, 271 (1951) (striking conviction for absence of permit where permit administration based only on custom). In Lakewood v. Plain Dealer Publishing, 486 U.S. 750 (1988), the Supreme Court struck down a law granting standardless discretion in the granting of annual permits for newsracks on public property. "[I]n the area of free expression a licensing statute placing unbridled discretion in the hands of a government official or agency constitutes a prior restraint and may result in censorship." Lakewood, 486 U.S. at 757; American Jewish Congress v. City of Beverly Hills, No. 93-55085 (9th Cir. July 19, 1996 (en banc), 96 Daily Journal D.A.R. 8705, 8708-9.

The AECA has no narrow, definite statutory standards. It states little more than a general policy to further "world peace and the security and foreign policy of the United States." 22 U.S.C. Sec. 2778(a)(1). No standards control what may be placed on the USML, because the USML simply consists of "'those items designated by the President" as being on the USML, 22 U.S.C. § 2794(7), and such designations are not "subject to judicial review." 22 U.S.C. § 2778(h). As a result, anything can be placed on the USML, and as previously explained, the licensing decision as to each applicant is also standardless. Thus the entire process is discretionary and presents a risk of censorship. The Government's treatment of PROF. BERNSTEIN and others demonstrates that this risk is not illusory.

B. The ITAR Scheme Relies On Content Evaluation By The Licensor.

The Lakewood court expressly relied on the problem of content evaluation in holding that an ordinance requiring annual permits for newsracks on public property required proper procedural protections. The annual renewal requirement permitted the licensor to measure the probable content or viewpoint of future expression by speech already uttered. Lakewood, 486 U.S. at 759- 760. Here, as described in page 23 *supra*, Defendants actually review speech about cryptography and appraise its possible uses, strength and effectiveness. Thus the ITAR Scheme presents a much more egregious content evaluation and should be struck down.

C. The ITAR Scheme Lacks The Freedman Procedural Safeguards.

In light of this Court's holding that source code is protected expression under the First Amendment, there can be no doubt that the standards of Freedman and Lakewood must be applied to the ITAR Scheme to the extent it controls speech. The prerequisites have been met: Defendants do not dispute that Plaintiff is subject to the regulations. Their letters to him require that he register as an arms dealer and apply for a license prior to the publication of Snuffle 5.0 and technical data related to it.

Finally, as explained below, even cursory review of the regulations reveals that they lack the procedural protections required by Freedman and its progeny. To be constitutional, the ITAR Scheme must "conform to procedures that will ensure against the curtailment of constitutionally protected expression," because "freedoms of expression must be ringed about with adequate bulwarks." Bantam Books, 372 U.S. at 66 (1963). It must operate under judicial superintendence and assure an almost immediate judicial determination of the validity of the restraint. Id., at 70 (footnote omitted). However, the major flaw in the ITAR Scheme remains its lack of enforceable standards. "Even if judicial review were relatively speedy, such review cannot substitute for concrete standards to guide the decisionmaker's discretion." Lakewood, 486 U.S. at 771.

1. There Is No Provision for Expeditious Judicial Review.

Essential to the scheme of procedural safeguards is expeditious judicial review; there must be a "prompt final judicial decision" reviewing any "interim and possibly erroneous denial of a license." Freedman, 380 U.S. at 59. "Because the censor's business is to censor . . . he may well be less responsive than a court . . . to the constitutionally protected interests in free expression." Id., at 57-58 (footnote omitted).

Neither AECA nor ITAR establishes any mechanism for judicial review of an interim restraint; in fact each purports to prohibit it. Once Defendants determined that Snuffle 5.0 was controlled, Plaintiff was no longer free to publish it. There must be judicial review of such a determination. Bantam Books, 372 U.S. at 71 (noting absence of "notice and hearing"). The Supreme Court has also added prompt appellate review to the Freedman list of procedural safeguards. Nat'l Socialist Party of America v. Village of Skokie, 432 U.S. 43, 44 (1977) (reversing state supreme court denial of stay of injunction against Nazi march). The ITAR Scheme plainly flunks this requirement as well.

2. There Is No Requirement for an Expedited Determination.

The failure to confine the time within which the censor must make a decision "contains the same vice as a statute delegating excessive administrative discretion." Freedman, 380 U.S. at 56-57. The ITAR scheme fails this requirement, because neither the CJ nor the licensing procedure contains any meaningful time limits. First, the CJ process provides at most that the applicant for a CJ determination may seek expedited processing if no decision has been rendered within 45 days.

Second, the CJ determination only establishes the need to apply for a license. The ITAR contains no time limit for license decisions. 22 C.F.R. § 126.7. One's application to publish under the ITAR, as with the application for a newspaper rack in Lakewood, "could languish indefinitely." Lakewood, 486 U.S. at 771. Indeed, even if a license is granted under the ITAR Scheme, it may be "revoked, suspended, or amended without prior notice." 22 C.F.R. § 126.7(a).

3. The Burden of Going to Court, And the Burden of Proof in Court Proceedings, Is on the Citizen Not the Government.

"[B]ecause only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint" Freedman, 380 U.S. at 58-59. "[T]he burden of instituting judicial proceedings, and of proving that the material is unprotected, must rest on the censor." Southeastern Promotions, 420 U.S. at 560.

AECA does not require Defendants to seek judicial review of their decisions to designate speech as controlled, or to deny a license for its publication. Instead, a speaker must, as Plaintiff has here, initiate legal action. Furthermore, because Defendants need not initiate judicial review, the AECA does not require Defendants to prove that the information may not be published. In fact, as shown above, the Government need not even explain their decisions until the discovery phase of formal litigation. This bureaucratic silence exacerbates the First Amendment problems. Lakewood, 486 U.S. at 769-70.

V. THE ITAR SCHEME IS UNCONSTITUTIONALLY VAGUE.

"[S]tandards of permissible statutory vagueness are strict in the area of free expression." Button, 371 U.S. at 432. Although usually framed in terms of fair notice, the more important aspect of vagueness is the requirement that a legislature establish minimal guidelines to govern law enforcement. Kolender v. Lawson, 461 U.S. 352, 358 (1983). Where expression is licensed, "[t]he vice . . . is particularly pronounced" because "available judicial review is in effect rendered inoperative" by lack of standards. Interstate Circuit v. Dallas, 390 U.S. 676, 683-685 (1968) (internal citations and quotations omitted). Thus, where First Amendment rights are involved, an even greater degree of specificity is required than the normal standard of adequate notice to a person of ordinary intelligence. Buckley v. Valeo, 424 U.S. 1, 77 (1976) (citations omitted). The ITAR Scheme falls well below the required standard. As we have seen, not even Defendants seem to know what their regulations include and exclude.

A. The AECA Lacks Standards Sufficient to Guide Administrative Discretion, to Aid a Court in Assessing the Exercise of Discretion or to Allow a Person To Know What the Regulations Regulate.

To the extent it licenses speech about cryptography, the AECA's lack of statutory standards, along with the unreviewability of USML designations, constitutes excessive discretion. The law requires "a precise statute evincing a legislative judgment that certain specific conduct be . . . proscribed . . . assur[ing] us that the

legislature has focused on the First Amendment interests and determined that other governmental policies compel regulation." Grayned v. City of Rockford, 408 U.S. 104, 109 n.5 (1972) (citation and quotation omitted). Congress has "impermissibly delegate[d] basic policy matters . . . for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application." Grayned, 408 U.S. at 108-09.

As noted above, the AECA provides no substantive standards for Defendants to follow or for a court to use in examining Defendants' exercise of that discretion to censor speech. Standards allow courts quickly and easily to determine whether the licensor is discriminating against disfavored speech. Without these guideposts, post hoc rationalizations by the licensing official and the use of shifting or illegitimate criteria are far too easy. Lakewood, 486 U.S. at 758.

Here the lack of standards has allowed Defendants to misuse a statute aimed at commercial, military arms sales to limit academic and scientific publication. Even the OLC has expressed doubt as to whether Congress intended to control any academic speech:

[i]t is by no means clear . . . that Congress intended that the President regulate noncommercial dissemination of information, or considered the problems such regulation would engender. We therefore have some doubt whether § 38 of the Arms Export Control Act provides adequate statutory authorization for the broad controls over public cryptography which the ITAR imposes.

Tien Decl., Exhibit A, Harmon Memo, at 4 n.7 (Bates stamp 60077). In a later memorandum, the OLC argued that "[t]he technical data provision received scant attention," and noted: "it does not appear that Congress addressed itself to the scope of §414 of the Mutual Security Act." Tien Decl., Exhibit C, Memorandum from Kathryn Fuller to Wayne Kay, at 2, 3 ("Fuller Memo"). The Fuller Memo continues:

[T]he legislative history underlying the authorization of regulation of 'technical data' provides little guidance as to the intended scope of that term. It seems clear that Congress contemplated the regulation of commercial exports of physical items such as blueprints and specifications. But it is not clear that Congress understood or intended its action to authorize controls over academic publication or oral communication of cryptographic ideas .... Although it might be argued that ... Congress was aware of and approved the existing provisions and interpretations of the ITAR, the sketchy and inconclusive legislative record pertaining to that section makes such an argument unpersuasive.

Tien Decl., Exhibit C, Fuller Memo, at 3-4. Thus the lack of standards for its application to protected expression, and indeed the uncertainty about whether Congress ever intended the AECA to be applied to protected expression, create constitutional vagueness in the AECA.

B. The ITAR Regulations Only Deepen The Vagueness.

The dangers of arbitrary and discriminatory enforcement against speech about cryptography created by the lack of standards in the AECA are manifest in the Government's implementation of the scheme. Defendants have defined "technical data" to include much scientific or technical information, including information about cryptography, and "export" to include all manner of communication and general publication. In reaching so broadly vagueness is enlarged by the ITAR, not confined.

1. The USML Is Vague.

Even what is considered "cryptographic" is not clearly defined in the ITAR Scheme. The USML prohibits items with "the capability of maintaining secrecy," 22 C.F.R. §121.1 XIII(b)(1). This clause gives little notice to the person of common intelligence, and lacks the "greater degree of specificity" required where speech is concerned. The Government itself recognizes and admits that the USML is vague by the very creation of the CJ Process. The CJ Process is to be used "if doubt exists as to whether an article or service is covered" by the USML. 22 C.F.R. § 120.4(a). Such a "doubt" is a constitutional flaw when speech is regulated.

2. The Categories of "Defense Articles," "Defense Services," and "Technical Data" Are Vague.

As previously noted at pages 5-8, the application and licensing requirements of the ITAR Scheme differ according to whether a defense article, defense service, or technical data is being exported. Yet each definition includes or is included by the other. *See* 22 C.F.R. § 123, 120.17(a)(1) (defense articles); 124, 120.17(a)(5) (defense services); 125, 120.17(a)(4) (technical data). When terms are cross-referenced this way vagueness persists until **each** term is narrowed. As also noted above, for this reason alone, Defendants'

reliance on Edler is misplaced; Edler only narrowed the definition of "technical data," leaving "defense articles" and "defense services" untouched.

The ITAR's treatment of software is vague for another reason. "Software" normally refers to expression in a computer language. Opinion at 29 nn. 3 & 4. But under ITAR, software "includes but is not limited to" logic flow and algorithms. 22 C.F.R. § 121.8(f). This definition has no limit and easily includes mathematical equations or diagrams. *Cf.* Gottschalk v. Benson, 409 U.S. 63, 65 (1972) ("algorithm" is "[a] procedure for solving a given type of mathematical problem."). Thus, contrary to normal definitions of "software" the ITAR definition could include virtually any discussion of how to solve a mathematical problem which Defendants might construe as "cryptographic."

3. The Exemptions are Vague.

The definition of technical data does exclude certain information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities. 22 C.F.R. 6§120.10(a)(5). This exemption only muddies the waters, however. What is a "general" principle; what does "commonly taught" mean? Suppose UC-Berkeley teaches a principle, but Stanford does not?

Similarly, "information in the public domain" is not technical data and is "not subject to the controls of this subchapter." 22 C.F.R. § 120.10(a)(5), 120.11, 125.1(a). Here lurks a subtle but critical Catch-22. To be "public domain," information must be "published" and "generally accessible or available" to the public in specified ways. 22 C.F.R. § 120.11(a). But publishing for the first time is "export". How can technical data become generally available "information" when publishing it for the first time is a prohibited export?

Furthermore, the Defendants' tortured interpretations of the ITAR create further uncertainties. For example, an ordinary person would believe that cryptographic source code could be "public domain," since it could be "information which is generally accessible or available to the public" under 22 C.F.R. §120.11 Yet Defendants apparently take the position that the public domain exception applies only to "technical data," despite the fact that it says it applies to all "information." Then they state that cryptographic software like Snuffle 5.0 is not technical data, and so cryptographic software can never enter the public domain. Demberger Decl. ¶¶ 3-4, 6-8.

This position is bizarre, because the definition of "public domain" only refers to "information." It does not mention "technical data." The definition of "technical data" uses the phrase "[i]nformation, other than software," implying that software is information. 22 C.F.R. § 120.10(a)(1). So Defendants apparently contend that software is information, but cryptographic software is not.

Whether or not Defendants' positions make sense, it is clear that the regulations fail to give fair notice of what is exempt. Equally important, they fail to confine Defendants' discretion as to what may be controlled and how. Such interpretive gerrymandering epitomizes the way a vague statute makes the use of "post hoc rationalizations" and "shifting or illegitimate criteria [] far too easy." Lakewood, 486 U.S. at 758.

In short, Defendants have defined "technical data" confusingly and defined exemptions from "technical data" vaguely. Even if each position were individually defensible, this system of regulation is as a whole too imprecise to pass First Amendment muster. *See* id., at 757, 769-70.

4. "Export" is Vague.

As noted above, AECA does not define "export"; the ITAR then creates a constitutional problem in this case by defining "export" to include communication and publication of speech about cryptography. No reasonable person would think that the statutory term "export" reached purely domestic communication of information. *See* United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989) (contrasting "export abroad" with "domestic disclosure"). Nor would a reasonable person think that "export" includes publishing information, even if that publication - like that of a newspaper or book or Internet publication - crossed the U.S. border. Indeed, if Congress had intended to reach publication, it could have done so explicitly in the AECA, as it has done in the espionage laws. *See*, *e.g.*, 18 U.S.C. § 794(b) (publishing defense information in wartime). Despite this, Defendants state that "posting cryptographic software and related source code to internationally distributed Usenet newsgroups on the Internet constitutes an export." Demberger ¶¶ 4, 10.

The circularity of the definitions of technical data, defense articles and defense services is crucial here, because whether a given action is an "export" depends on this categorization. *See supra* at pages 7-8. If you don't know which category your work is in, you don't know what counts as export and are left to guess. Speech cannot be punished when the rules are so unclear. *Cf*. Herndon v. Lowry, 301 U.S. 242, 261-63 (1937). As in the scheme requiring teachers to sign loyalty oaths in Keyishian, the ITAR Scheme is a

"regulatory maze" wholly lacking in terms susceptible of objective measurement in which vagueness of wording is aggravated by prolixity and profusion of statutes, regulations, and administrative machinery, and by manifold cross-references to interrelated enactments and rules. Keyishian, 385 U.S. at 604. As in Keyishian, the Scheme must be struck down.

VI. THE ITAR SCHEME IS OVERBROAD.

A licensing scheme is facially overbroad when it "does not aim specifically at evils within the allowable area of [government] control, but . . . sweeps within its ambit other activities that ... constitute an exercise" of First Amendment rights. Thornhill, 310 U.S. at 97. The danger is "not merely the sporadic abuse of power by the censor" but the "continuous and pervasive restraint on all freedom of discussion that might reasonably be regarded as within its purview." Id., at 97-98. Almost 20 years ago, OLC concluded that the ITAR scheme's licensing standards "are not sufficiently precise to guard against arbitrary and inconsistent administrative action." Tien Decl., Exh. A., Harmon Memo at 10 (Bates stamp 60083). In later memos, the OLC warned that the scheme's coverage was so broad that it could apply to "communication of unclassified information by a technical lecturer at a university or to the conversation of a United States engineer who meets with foreign friends at home to discuss matters of theoretical interest." Tien Decl. Exhibit A, 1984 ITAR Memorandum, page 2, (Bates Stamp 60007-8); *See* id. at pages 12-13 (Bates Stamp 60017-18).

The OLC was right. The problems they identified have not been remedied. The ITAR Scheme's broad definitions confer enormous discretion on Defendants, yet its terms provide that a court may not review a determination that academic publication of scientific speech must be licensed.

A. The Scheme Reaches A Substantial Amount Of Constitutionally Protected Activity.

As described in detail in Section I above, the ITAR Scheme reaches substantial First Amendment activities by both Plaintiff and others by licensing scientific and technical communication. *See* Village of Hoffman Estates v. Flipside, 455 U.S. 489, 494 (1982) (Court first determines if law reaches a "substantial amount of constitutionally protected conduct"). Equally important, Defendants have broad discretion to interpret the USML so as to require licensing of speech without fear of judicial review.

The Government has in practice exploited the overbreadth of the ITAR, even applying it to computer code which contains no cryptography at all. Mr. Brian Behlendorf maintains and develops the Apache server, a computer program which does not contain any cryptographic source code. Despite this, the Government has stated that it considers the program to be in violation of the ITAR. Declaration of Brian Behlendorf ("Behlendorf Decl."), ¶ 5. The Government's statement, carrying the implicit threat of prosection to the authors and maintainers of the program, is apparently based upon the fact that someone else could add cryptographic source code to the program and then have the ability to encrypt. Id., ¶¶. 5-10. As a result, with no proof whatsoever that the Apache computer code is either a defense article or "directly related" to an item on the USML as required by Edler, or that Mr. Behlendorf and his colleagues had any connection with foreign enterprises, the Government intimidated them into removing portions of the computer code from the Apache server. Behlendorf Decl., ¶ 8. The Government's acts have thereby both chilled and compelled Mr. Behlendorf's speech. Id., ¶¶ 8-11.

Thus, the scope of the ITAR Scheme, as applied by the Government, reaches beyond encryption source code to a much wider range of computer source code, including nearly all computer code which facilitates communication. Both on its face and as applied, it allows Defendants to require that authors of this computer code modify their ideas to fit the Government's will.

B. Edler Failed To Confine Defendants' Discretion

The Government has contended that the narrowing construction imposed by the Ninth Circuit in United States v. Edler Industries, Inc. cured any overbreadth problems in the ITAR Scheme. As described above, this contention is false, as even the OLC has acknowledged. Tien Decl., Exhibit D, Edler acknowledged that on its face, the definition of "technical data" is so expansive that if taken literally, it would require a license for the design principles of the diesel engine. Edler, 579 F.2d at 519, Such "expansive language may be construed to restrict . . . the interchange of scientific and technical information that of itself is without any substantial military application." Id. at 520. Thus, the Court sought to narrow the statute by requiring a "significant and clear" relation between the technical data and the production of an article on the USML. Id., at 520-21. It also imposed a scienter requirement for criminal liability for exports of technical data with peaceful uses. Id., at 521.

Unfortunately, Edler's narrowing construction has become meaningless. First, as noted above at Note 10 and Page 34, Edler construed only technical data and not defense articles or defense services. Here, Plaintiff's source code has been designated as a defense article, so Edler simply does not apply on its own terms. More generally, given the demonstrated vagueness and circularity of the current ITAR definitions, which were changed since Edler was decided, narrowly construing only one term like "technical data" does nothing to limit Defendants' discretion. For example, Defendants now apparently maintain that software generally is technical data - but that cryptographic software is not. They thereby escape Edler's restrictions by relabeling their terms. The government "cannot foreclose the exercise of constitutional rights by mere labels." Button, 371 U.S. at 429.

Second, even as to "technical data," Edler's narrowing effect has been eliminated as a practical matter by the subsequent elimination of judicial review of the regulatory designations of items as being on the USML in 22 U.S.C. §2778(h), which was also added after Edler was decided. As a result, a person charged with violating the ITAR cannot challenge Defendants' determination that an item was "significantly related to" an item on the USML. Regulatory language that apparently limits Defendants' discretion, such as the ITAR provision limiting application to items "specifically designed ... for a military application" (ITAR 120.3(a)), is similarly meaningless. As a practical matter then, whether information is controlled is completely up to Defendants. Edler's narrowing construction is unenforceable.

Defendants' application of ITAR to Plaintiff demonstrates that Edler did not fix the problem. In theory, Edler confined Defendants to "controlling the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise." Edler, 579 F.2d at 521 ("So confined, the statute and regulations are not overbroad."). If Defendants do follow Edler, their reading of it mocks the Ninth Circuit. Defendants assert that Plaintiff must get a license to publish Snuffle, even though he wishes to publish Snuffle as part of the scientific exchange of ideas and information extolled in Edler. Nor have Defendants disputed that cryptography, like much scientific and technical information, has important nonmilitary applications or that Plaintiff's intentions are nonmilitary and unconnected with any foreign enterprise. If Defendants truly followed Edler, they would not claim licensing authority over Plaintiff or any over general publication of such scientific information.

C. The ITAR Scheme Is Overbroad In That Its Broad Definition Of "Export" Prohibits General Publication and Public Discussion.

Plaintiff has shown that the ITAR Scheme is so broad that it even allows Defendants to regulate non-cryptographic computer programs as source code. Behlendorf Declaration, ¶¶ 5-10. The ITAR Scheme is also overbroad in that it applies to a broad range of communicative acts. *See supra* pages 9-10.

As Professor Nimmer has reasoned:

[w]here communicative activities occur with the intent to achieve a public disclosure to the American people (as distinguished from a private disclosure to an agent of a foreign nation), then it seems proper to conclude that such activities may be the subject of criminal punishment only if a 'serious injury' to the state can be proven both likely and imminent as a result of such public disclosure, as the Supreme Court has required in other free speech contexts.

Nimmer, "National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case," 26 Stan. L. Rev. 311, 331-32 (1974) (footnotes omitted).

The broad definition of "export" harms not only publishers but U.S. listeners as well. *See infra* at pages 14-15. Since any general publication of information -- whether in books, journals or electronic forums -- may be distributed internationally or will at least, possibly disclose that information to foreign persons in the US, general publication is an "export" for which a license is needed. Since the ITAR Scheme so discourages publication, U.S. listeners are deprived of valuable information. When PROF. BERNSTEIN may not speak, the rights of all who wish to hear him are also violated. This concern is particularly acute where, as here, the speaker is a teacher and the intended recipients are his colleagues and students.

D. The ITAR Scheme Is Overbroad in That it Assumes That All Foreigners Are Terrorists.

As noted in Section I.D above, the AECA prohibits granting export licenses to foreign persons. 22 U.S.C. § 2778(g)(5). There are no exceptions. Even a Nobel Prize winner in the United States, if a foreign person, may not get a license and so cannot teach a class containing foreign students or share with foreign colleagues any controlled information. Equally, because disclosure of technical data to foreign persons constitutes export for which a license is needed, every foreign person's right to receive information from a willing speaker is affected.

Plaintiff has already argued that the ITAR Scheme's discrimination against foreign persons violates the prohibition against content discrimination. Bellotti, 435 U.S. at 777 (1978). ("The inherent worth of speech ... does not depend on the identify of its source.") Even if it did not, however, blanket prohibitions based on foreign nationality are overbroad because not every foreign person poses the risk feared by the government. The ITAR Scheme is unconstitutionally overbroad not simply because it includes within its sweep some impermissible applications, but because in all its applications it operates on a fundamentally mistaken premise - that all foreign persons are a risk to national security. Munson, 467 U.S. at 965-66 (footnote omitted).

In Thornhill, an anti-picketing statute was held unconstitutional despite Alabama's undoubted interests in protecting against violence and breaches of the peace because that risk is not presented by every picketer; the law did not target serious encroachments or evidence care for the interest of the community and of the individual in freedom of discussion. Thornhill, 310 U.S. at 105. The law made "no exceptions" based on any number of circumstances relevant to the likely risk of picketing. Id., at 99.

Blanket assumptions about "the substantiality of the relationship between an individual and a group" are impermissible. Aptheker v. Secretary of State, 378 U.S. 500, 510 (1964) (crime for members of Communist groups to use or obtain U.S. passport); United States v. Robel, 389 U.S. 258, 265 (1967) (law imposing criminal penalties on Communists who got employment in a defense facility was overbroad because it "establishe[d] guilt . . . without any need to establish that an individual's association poses the threat feared by the Government in proscribing it.") (footnote omitted). These laws, like that in Thornhill, reached First Amendment activities without making exceptions where no genuine risk existed.

The ITAR Scheme functions the same way. Every disclosure of technical data to a foreign person requires a license. No foreign person can get a license. "Freedom of expression, and its intersection with the guarantee of equal protection, would rest on a soft foundation indeed if government could distinguish among [speakers] on such a wholesale and categorical basis." Mosley, 408 U.S. at 100.

CONCLUSION

There is no genuine issue of material fact that the ITAR Scheme creates a prior restraint on speech about cryptography, in requiring a license prior to publication or public communication of privately developed, unclassified cryptographic software, technical data and even such fundamental mathematics tools as algorithms, designs and logic flows. There is no genuine issue of material fact that, even absent the censorship scheme, the ITAR Scheme punishes U.S. citizens for engaging in speech about cryptography. As a result, longstanding U.S. Constitutional law mandates that the ITAR Scheme pass both the prior restraint test of Pentagon Papers and the strict scrutiny tests. Plaintiff submits that these tests cannot be applied without discovery as to the damage caused by publication, the Government's interests, and the fit between those interests and the regulatory scheme and the existence of less restrictive means, among others.

As to the procedural protections required by the First Amendment however, there is no need for discovery. There is no genuine issue of material fact that the ITAR Scheme, to the extent it controls speech about cryptography, falls far short of the minimum requirements for speech licensing schemes. Indeed, the undisputed facts demonstrate that the ITAR Scheme is a Kafkaesque procedural labyrinth pervaded by unfettered discretion and delay. First Amendment law requires a much more precise and protected scheme before scientific speech can be properly regulated. On this ground alone, Plaintiff urges this Court to invalidate the ITAR Scheme to the extent it reaches speech about cryptography, including source code.

In addition, while the lack of procedural protections in the ITAR Scheme is a critical violation of the First Amendment , the ITAR Scheme is a prior restraint which cannot be saved by procedural safeguards alone. Given the vagueness and facial and applied overbreadth of the ITAR Scheme, it is guaranteed to sweep more widely than its stated purpose of preventing "the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise." Edler, 579 F.2d at 521. As the Supreme Court long ago observed: [T]o the extent that vague standards do not sufficiently guide the censor, the problem is not cured merely by

affording de novo judicial review. Vague standards, unless narrowed by interpretation, encourage erratic administration whether the censor be administrative or judicial; 'individual impressions become the yardstick of action, and result in regulation in accordance with the beliefs of the individual censor rather than regulation by law[.]'

Interstate Circuit, 390 U.S. at 685 (quotations omitted)

The preclusion of judicial review under 22 U.S.C. § 2778(h) magnifies every defect in the scheme. As demonstrated above, it defeats judicial attempts to narrow the scope or application of the ITAR Scheme, since the required findings and showings by the Government are fundamentally unenforceable and the agency retains unbounded discretion.

Accordingly, the statute must be invalidated on its face.

Dated:_____ Respectfully submitted,

McGLASHAN & SARRAIL
Professional Corporation

By:_____
CINDY A. COHN