IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DANIEL J. BERNSTEIN Plaintiff/Appellee, v. David J. Bernstein UNITED STATES DEPARTMENT OF JUSTICE, et al., Defendants/Appellants	)	No. 97-16686 C-95-0582 MHP (N.D. California, San Francisco)

BRIEF FOR THE APPELLEE

CINDY A. COHN, ESQ.; SBN 145997
McGLASHAN & SARRAIL
Professional Corporation
177 Bovet Road, Sixth Floor
San Mateo, CA 94402
Tel: (650) 341-2585
Fax: (650) 341-1395

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

M. EDWARD ROSS, ESQ.; SBN 148216
STEEFEL, LEVITT & WEISS
A Professional Corporation
One Embarcadero Center, 30th Floor
San Francisco, CA 94111
Tel: (415) 788-0900

DEAN MOREHOUS; SBN 111841
SHERI A. BYRNE, SBN to be assigned
THELEN, MARIN, JOHNSON & BRIDGES
2 Embarcadero Center, 17th Floor
San Francisco, CA 94111
Tel: (415) 392-6320

LEE TIEN, ESQ.; SBN 148216
1542 Curtis Street
Berkeley, CA 94702
Tel: (510) 525-0817

ROBERT CORN-REVERE, ESQ.
HOGAN & HARTSON, L.L.P.
555 Thirteenth Street, N.W.
Washington, D.C. 20004
Tel: (202) 637-5600

Attorneys for Appellee
DANIEL J. BERNSTEIN

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Other Materials

INTRODUCTION

The Supreme Court calls the Internet a "unique and wholly new medium" that "enables tens of millions of people to communicate with one another and to access vast amounts of information from around the world. . . . At any given time, tens of thousands of users are engaging in conversations on a huge range of subjects. . . .The content on the Internet is as diverse as human thought." Reno v. ACLU, 117 S. Ct. 2329, 2334-35 (1997) (citations and internal quotations omitted). ("Reno") But from this diversity of content and speakers, the government has chosen one subject--cryptography, the science of speech privacy--and one group of speakers--U.S. persons--for exclusion from "the most participatory form of mass speech yet developed." Reno, 117 S. Ct. at 2340 (citations omitted).

Plaintiff Daniel J. Bernstein is a professor in the Department of Mathematics, Statistics and Computer Science at the University of Illinois at Chicago.1 Writing, analyzing and publishing cryptographic algorithms and software is integral to his academic research and teaching. It is also plainly protected speech. Software in the form of source code was designed to be read and understood by humans and is a critical tool in teaching on subjects involving computers. It is as difficult to develop the science of cryptography without reading software as it would be to develop poetry without reading poems or the theory of relativity without reading mathematical equations. The undisputed impact of Appellants' cryptography regulations, however, is to subject Professor Bernstein and others to criminal prosecution for publishing their work on the Internet without receiving an "export" license.2

The Government asserts that this restraint on scientific work is necessary to prevent foreign intelligence targets from getting cryptographic information which they might then use to make it more difficult for the Government to eavesdrop on their communication. But the regulations are so clumsily written that they do not even achieve this end. For even while they license academics like Professor Bernstein's electronic publication, they do not license any print publication of cryptographic information. As a blue-ribbon commission assigned by Congress to examine the cryptography regulations3 noted, the academic community greeted the government's rules with the comment: "They think terrorists can't type?" Bernstein v. Department of State, 945 F. Supp. 1279, 1296, n.10 ("Bernstein II")

Even worse, the Government has known for 20 years that these regulations are an unconstitutional prior restraint. The Justice Department's Office of Legal Counsel ("OLC") in 1978 clearly and succinctly outlined the basic failure to provide limitations on agency discretion and procedural protections that plague the scheme today.4 The District Court's reasoning below, for all practical purposes, adopts the OLC's reasoning.

At bottom, these regulations create a highly discretionary licensing scheme aimed at an entire subject area of science--an obvious prior

restraint. The government's justification hangs in the air, unsupported by evidence and undercut by its own exemptions. As the Supreme Court said in Reno, "[t]he interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship." Reno, 117 S. Ct. at 2351.

II. ISSUES ON APPEAL

The issues presented on appeal are whether the District Court correctly held that the cryptography regulations are a facially unconstitutional prior restraint on speech and whether the relief granted was proper.

III. STATEMENT OF THE CASE

A. BACKGROUND

Cryptography has been used in communication for more than 3,000 years, and has a long and prestigious history of use in the United States.5 Colonial patriots frequently used cryptography.6 Exchanging views on politics, philosophy and constitutional theory, Thomas Jefferson and James Madison corresponded in code "so thoughts they exchanged would not fall into the hands of political foes."7 In sharp contrast to the government's position in this case, the American Founding Fathers viewed secret writing as an essential instrument for protecting critical information not only in wartime, but in peacetime, as well.8 Today, as a branch of applied mathematics, cryptography is still used to protect the privacy of messages and stored information. Appellants' Excerpts of Record ("ER") 300. As in the Framers' times, it is a science that aids interpersonal communication. AER 8-9; 78-9; 139-40; 146-7; 154-6; 180-9; 191-4. Without cryptography, for example, electronic mail is like a postcard, open to view while the message is in transit. See ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996) (finding 23) aff'd Reno. With cryptography, people can put messages into electronic "envelopes." See Bruce Schneier, E-Mail Security (1995). The uses of cryptography today include protecting the privacy of attorney/client correspondence, financial transactions, political discussions, medical records, human rights reports and cellular telephone conversations. Continued development of cryptography may enable the Internet to offer private communication among billions of people worldwide. AER 78-80; 139-40; 189; 192-4; 196. Despite cryptography's growing importance to all who communicate electronically, the Government has long used export restrictions to restrain its development by private citizens, including academics.9 In the mid-1980s, for example, a number of scientific meetings were disrupted by National Security Agency threats of prosecution for violation of export control laws.10 A congressional study of the NSA's efforts during this period concluded that "[c]ontrols over the export of unclassified technical data pose a constant threat to [private use and development of] cryptography."11 Censorship of academic speech about cryptography has continued. The record below contains several recent examples in which the administrators of the export control regime informed scholars that licenses are required for academic activities involving cryptography (AER 175-6) and declined to provide clear guidance when asked about the status of a class project.12 (AER 151-3). When MIT Press asked if it could publish an academic book containing cryptographic source code, the Government opened a case file, delayed for months, then ultimately refused

to respond. AER 331-335. Most recently, the FBI and others have advocated additional statutory domestic controls over the distribution and use of cryptography.13 It is in this context that the District Court found that the cryptography regulations' prepublication licensing requirements are facially unconstitutional.

B. The Cryptography Regulatory Scheme

When this case began, all cryptographic speech export was controlled by the State Department under the ITAR scheme.14 It was under ITAR that Appellants made the initial determinations about Professor Bernstein's request to publish and the District Court decided Bernstein I15 and Bernstein II. On December 30, 1996, primary licensing authority for nonmilitary cryptography was shifted to the Commerce Department.16 Appellants have admitted that Professor Bernstein would need a license under the new regulations, stating: "the parties' dispute as to licensing procedures for Professor Bernstein's encryption source code, and as to technical data, would continue." AER at 477-84. Under both the cryptography regulations and the previous ITAR scheme, a person wishing to publish encryption software and related "technology"17 must apply for and be granted a license prior to electronic publication, because such publication is defined as "export." Even disclosing technology to a foreign person within the United States is defined as an export. 15 C.F.R. ß 734.2(b)(3)(ii). In addition, a person must also get a license to provide "technical assistance" about encryption to a foreign person. 15 C.F.R. Sect.744.9(a).

1. The Licensing Process

The cryptography license application process requires that a person submit the speech to be communicated for review by agency officials. Those officials read and evaluate the submission and then decide whether to permit or deny a license, or that no license is needed. Importantly, under the cryptography regulations, license decisions are made "on a case by case basis." 15 C.F.R. Sect. 742.15(b)(4)(ii) and there are no substantive standards for agency decision making. Penalties for "exporting" controlled items without a license include up to $250,000 in fines and up to ten years in prison. 15 C.F.R. Sect. 764.3 & 6.4. Within 90 days, initial license applications are decided by the Commerce Department or referred to the President. 15 C.F.R. Sect. 750.4(a). If an application is referred to the President, he or she has no deadline for decision. If a license is denied, an appeal can be taken within Commerce. 15 C.F.R. Sect. 756.1(a). There is no deadline for Commerce to decide an appeal, however; appeals need only to be decided "within a reasonable time." 15 C.F.R. Sect. 756.2(c)(1). During the internal appeals process, the licensing denial remains in effect, and the work cannot be published or otherwise "exported." 15 C.F.R. Sect. 756.2(d). Judicial review of licensing decisions is expressly precluded under the EAA and EAR. 50 U.S.C. App. Sect. 2412 and 15 C.F.R. Sect. 756.2(c)(2). While IEEPA does not preclude judicial review,18 it fails to require: (1) that such review be prompt or (2) that the government bring the action and bear the burden of proof.

2. The Cryptography Regulations Differ Significantly from the General EAR Licensing Process

The cryptography regulations differ from the broader EAR regulations in several ways, demonstrating that the topic of encryption is singled out for more restrictive treatment than other scientific topics subject to the EAR. First, "export" is defined separately for speech about cryptography expressed in a programming language than for any other kind of speech licensed by the EAR. For all other speech, "export" is defined as communication to anyone in a foreign country or to a foreign person in the United States. 15 C.F.R. Sect. 734.2(b)(2),(3). For speech in the form of encryption software, however, the term "export" expressly includes Internet publication:

> downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States . . . unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States.

15 C.F.R. Sect. 734.2(b)(9)(B)(ii). No other speech, regardless of its subject matter or "capability" is so heavily burdened. Second, the First-Amendment-sensitive exceptions applicable to all other software are inapplicable to encryption software. These exceptions allow "export" without a license of software that results from "fundamental research," (15 C.F.R. 734.3(b)(3)(ii) and 734.8); that is "educational" (15 C.F.R. 734.3(b)(3) (iii) and 734.9), and that is "publicly available." In addition, the EAR excludes from licensing items that are already available from foreign sources (15 C.F.R. Sect. 768) and items that have de minimis U.S. content (15 C.F.R. Sect. 734.4). None of these exceptions are applicable to cryptography.19 These extra restrictions create some absurd results. For instance, a person needs a license to publish software on a U.S. Internet site even if it is already freely available from an Australian site.20

C. How the Cryptography Regulations Were Applied to Professor Bernstein

This case fundamentally presents a facial challenge. The facts of Appellants' treatment of Professor Bernstein contained in the record, however, illustrate the unbridled administrative discretion conferred by the export regulations. They also show how that discretion has been used in erratic, inconsistent and plainly wrong ways to restrict the free flow of information about the subject of cryptography by scientists and academics. As a student, Professor Bernstein developed an encryption algorithm21 which he named "Snuffle." He then described his algorithm in two ways: in a scientific Paper containing both English and mathematical equations (hereinafter the "Paper") (AER 3) and in a computer program in the "C" programming language (hereinafter "Snuffle.c") (AER 4 & 5). Later, he wrote instructions in English explaining how to use Snuffle to encrypt and instructions in English for programming a computer to use Snuffle (collectively referred to hereinafter as "Instructions").22 Like most scientists, and especially those who live in the "publish or perish" environment of academia, Professor Bernstein sought to present his idea to the worldwide academic and scientific community using the normal channels of

discussion and publication. Vaguely aware of Appellants' restrictions on cryptography, Professor Bernstein asked the State Department (which administered the export regulations at that time) whether he needed a license to publish his work, initially consisting of Snuffle.c and the Paper. AER 1-5, 18-19. The State Department responded by indicating that Professor Bernstein did need a license. AER 20. Professor Bernstein then engaged in a protracted, frustrating and ultimately unsuccessful attempt to learn how Appellants interpreted their regulations and whether the determination extended to both the source code and his scientific Paper expressions of the Snuffle algorithm.23 AER 10-15,21-41. At one point, for example, he was told he could be prosecuted for placing his work into a public library. AER 26. Professor Bernstein appealed the licensing determination on September 22, 1993. AER 14 and 21. He never received a response. AER 14-15. More than two years later and after this suit was filed, however, Appellants' issued a "clarification" indicating that the scientific Paper was not controlled. AER 14-15, 42-44.24 However, Snuffle.c and the Instructions, which he had submitted later, remain restrained.25 AER 479. Appellee's frustrating experience is by no means an isolated instance. AER 147-55; 175-6; 141-3; 184-5; 500-6 and NRC Report 4-14 to 4-18, 4- 30 to 4-33 and 4-47.26

IV. SUMMARY OF ARGUMENT

The Government has prevented Professor Bernstein and many other academics and scientists from effectively teaching and publishing about the mathematical field of cryptography. Writing and analyzing cryptographic algorithms and software is integral to scientific and academic work on this topic. Such software is a creative achievement by its author, is often read and evaluated by his colleagues and students, and so easily falls within the ambit of the protections the Supreme Court has long accorded speech in its many forms. The fact that Professor Bernstein and others wish to publish on the Internet makes no difference to the analysis of this situation. The Supreme Court has recently recognized that the Internet is a fully protected medium for First Amendment expression. The District Court, agreeing with a 1978 OLC analysis of the regulations, held that they are an illegal prior restraint. That decision was clearly correct: the regulations have more than a close enough nexus to speech to pose risk of censorship, they directly restrict scientific speech in a particular subject area of applied mathematics, specifically prevent such speech on the Internet, and restrict private communication. Further, the regulations grant unfettered discretion to the bureaucrats who implement it, and lack the procedural safeguards required by Freedman v. Maryland, 380 U.S. 51 (1965). The lack of narrow, definite and objective standards causes self-censorship and permits unreviewable content-based discrimination, both of which are demonstrated in the record. The Government misapplies the First Amendment framework by presenting content-neutrality as the necessary threshold question for this review. This argument is flawed because prior restraints are invalid even when content-neutral, and, in any event, the cryptography scheme is content-based. Further, the government has failed to prove that its interest in national security is furthered in any material way by the licensing scheme, and indeed its assertions here are undermined by both common sense and its own Congressional testimony on the subject.

Moreover, even under the more forgiving standard that governs certain content-neutral restrictions, the cryptography scheme is defective. It reaches overbroadly and is fatally imprecise. Finally, the District Court granted the proper scope of relief; its decision should be affirmed in its entirety.

V. ARGUMENT

A. THE EXPORT CONTROLS ON CRYPTOGRAPHIC SPEECH ARE AN UNCONSTITUTIONAL PRIOR RESTRAINT 27

Under the cryptography regulations, Professor Bernstein must not take or send Snuffle 5.0 abroad in any manner, except for personal use. See 15 C.F.R. Sect. 734.2(b)(1). He must not present Snuffle 5.0 at a conference abroad or communicate it privately to an overseas colleague (even a U.S. citizen). See 15 C.F.R. Sect. 734.2(b)(2). He must not present his work or discuss its merits in the Internet newsgroup "sci.crypt" (see 15 C.F.R. Sect. 734.2(b)(9)(B)(ii)), or publish his ideas in an electronic scientific journal such as the American Association for the Advancement of Science ("AAAS") journal Science. Id. In short, Professor Bernstein may not engage in forms of scholarly dialogue that have become commonplace in virtually every other field of academic pursuit. Unless, of course, he obtains the government's permission first. This is prior restraint in its classic form.

1. Prior Restraint Analysis Applies to Discretionary Licensing Regulations That Target Speech, Regardless of Content Neutrality

The fundamental issue in this case is whether the government's licensing scheme over encryption software, related technology and technical assistance is subject to a facial challenge as an unconstitutional prior restraint. As correctly determined by the District Court and as conceded by the Government on appeal, the appropriate test for resolving that issue is Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750 (1988). Appellants' Brief at 39. The relevant question is whether the cryptography licensing scheme has a "close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of the identified censorship risks." Id. As demonstrated below, the answer is yes. The cryptography scheme is a direct restriction on speech, whereas the Supreme Court in Lakewood found a "close enough nexus" when regulations merely controlled the vending machines used to distribute speech. A licensing statute that restricts speech and places unbridled discretion in the hands of the administering government agency is a prior restraint. See Lakewood, 486 U.S. at 757. As the District Court correctly observed, the cryptography regulations impose no limits on agency discretion. Bernstein III, ER 570. They are therefore a prior restraint and subject to a facial challenge. The next step of the analysis, also correctly determined by the District Court, is simply to apply the factors governing prior restraints articulated in Freedman v. Maryland: 1) whether the agency is required to make expedited decisions; 2) whether expeditious judicial review is available; and 3) whether the censor bears the burden of going to court and has the burden of proof. See, e.g., Freedman, 380 U.S. at 58-60. The cryptography scheme clearly fails to satisfy even one of these requirements, and Appellants do not defend the rules on this basis. The District Court correctly determined

that the cryptography regulations fail the Freedman test and concluded that it need look no further. See Bernstein III, ER 569 and 578, citing FW/PBS, Inc. v. Dallas, 493 U.S. 215, 236 n.3 (1990) ("In light of our conclusion that the licensing requirement is unconstitutional because it lacks essential procedural safeguards . . . we do not reach [the other First Amendment challenges to the ordinance's licensing scheme]"). If this Court agrees that Freedman and its progeny establish the relevant tests in this case, it may make short work of the government's appeal, for Appellants essentially have admitted that the cryptography scheme cannot survive rigorous constitutional scrutiny. The Government attempts to bypass this straightforward analytical framework by contending that "content - neutral regulations are constitutional as long as they serve substantial interests that are unrelated to the suppression of speech and they do not incidentally burden substantially more speech than necessary." Appellants Brief at 30. The necessary but unstated premise to the Government's argument is that if the regulations at issue pass the "content neutrality" and "unrelated to the suppression of speech" tests, then no prior restraint facial challenge to the regulations will lie. Beyond the fact that the government is advocating the wrong First Amendment test, there are two major problems with its analysis: the cryptography regulations are not content-neutral, and even if they were, the Freedman requirements still apply. The cryptography regulations on their face target speech about the topic of cryptography.28 "[T]he 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 (1992) (citation and footnote omitted); accord, Simon & Schuster, Inc. v. Members of the New York State Crime Victims Board, 502 U.S. 105, 116 (1983) (statute restricting speech about crime is content based). As explained above, the exemptions designed to protect First Amendment speech that apply to all other software are specifically do not apply to software with cryptographic content. These exemptions include publicly available software, foreign available software, educational software and software resulting from fundamental research. See supra at 12-3. Additionally, cryptography is subject to a special licensing requirement for "technical assistance" which has no counterpart elsewhere in the EAR scheme. 15 C.F.R. Sect. 744.9(a). Clearly the cryptography scheme is not neutral on the subject of cryptography. The Government's repeated assertion that the District Court found that the "licensing requirements are content-neutral regulations that are not aimed at the suppression of speech" (Appellants' Brief at 17 & 36) is flatly wrong. The District Court found that the regulations were aimed at the suppression of speech. Bernstein III, ER 567. ("The encryption regulations . . . [are] specifically directed at speech protected by the First Amendment."). What the District Court found, and what the government fails to acknowledge, is that the question of content neutrality is irrelevant to prior restraint analysis. See Bernstein III, ER 569 ("thus, without deciding whether the regulations are content based, the court turns to the procedural safeguards afforded under the encryption regulations"). The District Court simply applied settled law that even neutral licensing schemes are unconstitutional prior restraints if they give government officials discretionary power to burden speech. Lakewood, 486 U.S. at 759; see also FW/PBS, 493 U.S. at 229 (plurality opinion) (finding that under ordinance city did not pass judgment on content of protected speech, but had indefinite amount of time to issue license). That Appellants' justification may be content-neutral does not address the special concerns of licensing

schemes: discriminatory application. The newsrack permitting scheme in Lakewood was neither facially content-based nor justified in terms of content, but it could be applied discriminatorily. Lakewood 486 U.S. at 757-759 (dangers of self-censorship, censorship, unreviewability, and irretrievable loss of speech opportunities are produced by "lack of express standards"). The record evidence of Appellants' treatment of Professor Bernstein, Mr. Miller, MIT and many others demonstrates that such dangers have been realized in the Appellants' application of the cryptography regulations. See supra at 7; AER 81-3; 84-102; 138-43; 144-72; 173-78; 179-89; 191-202; 333-40; 490-99; 500-18.

2. The Cryptography Regulations Regulate Expressive Activity

The Government does not deny that Professor Bernstein needs a government license. It very frankly admits that "source code can be understood by persons, such as computer scientists and programmers."29 Thus it admits that the cryptography regulations directly regulate the "expressive activities" of computer programmers, scientists, academics and others. Appellants' Brief at 41. It admits that the regulations restrict Professor Bernstein's expressive activities "even if his own purpose is merely to convey some theory implicit in the software."30 These admissions alone demonstrate that the scheme has a "close enough nexus to expression" to trigger facial prior restraint review under Lakewood. The government's defense of the cryptography scheme is premised on the improper (and unproven) factual assumption that the electronic publication of encryption source code and related information is very rarely, "if ever" (Appellants' Brief. 28) done for expressive purposes. Not only is this assertion undermined by the government's own admissions, the error was exposed by the court below. The District Court found that "[b]y the very terms of the encryption regulations, the most common expressive activities of scholars - teaching a class, publishing their ideas, speaking at conferences, or writing colleagues over the Internet - are subject to a prior restraint by the export controls when they involve cryptographic source code or computer programs." Bernstein III, ER 566. The District Court further found that the cryptography regulations "threaten to undermine the essential features of scientific freedom and the open exchange of information that are generally acknowledged as critical to innovation in science and technology." Id. at 567 (quoting AAAS statement). Academic freedom is "a special concern of the First Amendment."31 Thus, it is not accurate to characterize the export controls as regulating "conduct commonly associated with speech," or as an "incidental" restriction on speech. The controls focus directly on an important form of academic and scientific communication. The cryptography regulations are a censorship scheme that must receive the strictest judicial scrutiny, not the attenuated review proposed by the government. The cryptography scheme directly impedes speech in three significant ways. First, it directly restricts the languages of the scientific dialogue. Second, it limits the media by which the speech may be conveyed. Third, the scheme impedes the ability of all Americans to communicate using encrypted speech.

a. The Regulations Restrict Communications Written in Programming Languages

As demonstrated by Appellants' admissions that programming languages,

including source code, are important means of communication for computer scientists and academics, the cryptography scheme imposes a direct burden on protected expression. A national commission recognized years ago, "[C]omputer programs are a form of writing. . . . The instructions that make up a program may be read, understood, and followed by a human being."32 As a form of language, computer code is inherently expressive, and therefore protected by copyright, thus lending further support for the conclusion that computer programs are protected by the First Amendment. 33 Just as composers use the specialized language of musical notation to specify what notes are to be played when, computer programmers use specialized languages familiar to their audiences to communicate precisely. Professors Abelson and Sussman of the Massachusetts Institute of Technology have explained that programming languages speak to people as much as they speak to computers:

> 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 AER 965-69. Similarly, the author of the seminal work on computer programming, Professor Donald E. Knuth of Stanford University, wrote: "Programming is best regarded as the process of creating works of literature, which are meant to be read . . . 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." Donald E. Knuth, Literate Programming, preface, ix (1992). See AER 73-4; 104-6; 108-9;124-5; 140-141; 183-86, 188; ER 301. For this reason, articles and papers containing and discussing cryptographic algorithms, source code and theories have been published in scientific journals for over 25 years for peer review and evaluation. ER 301 (Joint Statement); see also AER 106-8. While some computer languages are more difficult for lay people to read, others are very close to standard English. An example of the latter is the program that can calculate the date of Easter for any given year. It contains simple, readable instructions such as "Divide year by 100 giving century." AER 573.34 While not denying the inherently communicative nature of computer language, the government asserts that it has no intention of restricting such communication. Instead, Appellants seek to diminish the level of First Amendment scrutiny in this case by claiming that the cryptography scheme is "not aimed at preventing the free exchange of information and ideas about cryptography," but seeks only to regulate cryptographic software because of its "capacity" (called "functionality" by the government below). The scheme, according to this argument, distinguishes between the control of "encryption products" and "cryptographic information." Appellants' Brief at 29 (emphasis in original). This argument is pure semantics. Where, as here, government action directly restricts protected speech, the government's good intentions are irrelevant. Minneapolis Star & Tribune Co. v. Minnesota Commissioner of Revenue, 460 U.S. 575, 592 (1983) (illicit legislative intent is not the sine qua non of a First Amendment violation). In addition, the government's argument is based on a false dichotomy. That the

cryptography scheme exempts the communication of source code when written on paper (evidently because such distribution is part of the "public dissemination of cryptographic knowledge," Appellants' Brief at 38), applies it to the identical information when published on the Internet or on a floppy disk (evidently turning the "speech" into a "product") reveals that there is no difference in the government's distinction. Information in either form can be used to make a computer operate, and perhaps for that reason Appellants "reserve[d] the right to control scannable source code."35 Further, most speech has the "capacity" to do something. Political speech has the capacity to spur people to vote or to protest; parody has the capacity to inflict emotional distress; even truthful speech has the capacity to damage reputation. Much speech that we describe in terms of content can also be characterized in terms of "capacity." On Appellants' view, such regulation would escape strict scrutiny. See Forsyth County v. Nationalist Movement, 505 U.S. 123, 134 (1992) (permit fee based on the capacity for a march to cause violence was content-based). The government attempts to distinguish cryptographic "products" from "speech." However, similar First Amendment "distinctions" when applied to communications media have been debunked over time. For example, the cinema is now fully protected under the First Amendment. This was not always the case, however. Initially the Supreme Court denied constitutional protection by applying the same distinctions the government advocates here: that "the exhibition of moving pictures is a business, pure and simple,"36 (i.e., a "product" as opposed to "speech") and it is "capable of evil, having the power for it, the greater because of their attractiveness and manner of presentation" (i.e., it has greater "capacity").37 The Court ultimately overruled this analysis38 and now treats film as "one of the traditional forms of expression such as books" that are protected as "pure speech."39 Finally, because computer programs are sets of instructions,40 the government cannot control what those instructions do without also controlling what they say. See Appellants' Brief at 28. Like a regulation that would prevent composers from exchanging sheet music or a recording of a composition, the cryptography regulations fundamentally alter the substance of academic exchange. It is not the same, for example, to allow the composers freedom to exchange written essays on music theory - the melody would be lost. For that reason, it is the "usual rule that governmental bodies may not prescribe the form or content of individual expression." Cohen v. California, 403 U.S. 15, 24 (1971). It is not possible to restrict the form of expression "without also running a substantial risk of suppressing ideas in the process." Id. at 26. The cryptography regulations on software do just that.

b. The Regulations Restrict Internet Publication

The export controls also significantly restrict the way in which scientific exchange takes place. The government admits that computer scientists and programmers commonly publish their programs electronically on the Internet41 to engage in the scientific exchange of ideas and information. ER 302 (Joint Statement). 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." AER 15; 16; 73; 76. In essence, science itself is a worldwide web of conversation among scientists. A scientist like Professor Bernstein publishes an idea in any of these fora, expressed in source code, mathematics or any language he deems appropriate.

Others -- academics, commercial scientists, or hobbyists -- then read or test his work, perhaps publishing their own comments or improvements, thereby continuing its development. Like many others in the record,42 Dr. Ginsparg of Los Alamos Labs, confirmed that "these systems and discussion groups are a fundamental part of the development of science. They are the natural extension of, and I believe the successor to, print publication of ideas." AER 124. Professor Bernstein seeks to publish his ideas in "sci.crypt," an Internet "newsgroup" or informal discussion group about cryptography.43 He also wishes to publish his ideas in more traditional academic journals. Yet an increasing number of journals like the AAAS publication Science, formerly available only on paper, are now also electronically available on the Internet. In fact, AAAS has publicly warned that the cryptography regulations affect Science because it is published in both print and electronic form. ER 566-7. Professor Bernstein also seeks to share his ideas by teaching, another activity which today often involves the Internet. AER 16-17. University classes in computer-related fields often have course syllabi, assignments, and materials available on the Internet, see Reno, 117 S. Ct. at 2334 (colleges and universities provide Internet access to students and faculty);44 some require students to publish on the Internet. AER 145. In the case below, the government argued that it should be able to prosecute Professor Bernstein if he placed his course materials -- which included cryptographic software -- on the University of Illinois Web site as part of the process of distributing course materials to his students.45 Finally, Professor Bernstein must be free to share his ideas with colleagues before he decides whether to publish them; 46 academic freedom embraces one-to-one exchanges of ideas and information with one's colleagues.47 Appellants claim that they do not restrict academic speech because "the EAR excludes books, magazines, and other printed materials on all subjects, thereby giving carte blanche to the export of publications on cryptography." Appellants' Brief at 29. But these regulations plainly do not give carte blanche. If Professor Bernstein uses paper, he can publish and exchange software. But if he wishes to use the Internet, he cannot publish or exchange software. Far from giving carte blanche, the government is actively restricting a medium recently found to be entitled to maximum First Amendment protection. Reno, 117 S. Ct. at 2344. The Reno Court emphatically rejected the argument that a law could "effectively censor[] discourse on many of the Internet's modalities" so long as it permitted speakers a "reasonable opportunity" to engage in speech in other areas.48 The Court found this argument to be "equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books," and it reaffirmed the bedrock principle that "'one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place.'" Id. at 2348-49, quoting Schneider v. State, 308 U.S. 147, 163 (1939). See also Lakewood, 486 U.S. at 762 (holding as "meaningless" the distinction of distributing newspapers "by a machine rather than by hand").

c. The Regulations Restrict the Ability to Encrypt Speech

Appellants claim broad ability to regulate cryptography because it can make speech private. But this characteristic of encryption technology is another reason why the government's actions are subject to First Amendment scrutiny.49 Federal law describes cryptography as method of secret writing.50 The Supreme Court has long considered individual privacy in

communications to be a core element of freedom of speech. For example, the Court has established that "[t]he right to speak and the right to refrain from speaking are complementary components of the broader concept of 'individual freedom of mind.'"51 Freedom from compelled speech is a "fixed star in our constitutional constellation."52 A related line of cases holds that the First Amendment includes the right to teach a foreign language.53 Yet another line of authority directly addresses the First Amendment right to speak anonymously. 54 Following the same principles, the Supreme Court has struck down state laws that required members of groups to reveal their identities.55 In each of these First Amendment contexts, the government advanced powerful justifications to restrict speech, yet the courts held that they were insufficient to overcome constitutional protections for privacy and speech. Here, Appellants raise a number of national security claims, but they must overcome the fact that encrypted speech is nevertheless speech. See McIntyre v. Ohio Elections Commission, 115 S. Ct. at 1524 ("our society accords greater weight to the value of free speech than to the dangers of its misuse"), citing Abrams v. United States, 250 U.S. 616, 630-631 (1919) (Holmes, J., dissenting). Given this background, the government may justify encroachments upon the ability to encrypt speech only upon a compelling showing of need. It may be true that the constitutional status of cryptography presents a "novel" question. Appellants' Brief at 24. It is novel, however, only in that it has not been previously litigated -- the First Amendment principles involved are well established. The Supreme Court confronted a similar situation involving the Fourth Amendment in 1928 when it first confronted the constitutional status of wiretapping. In Olmstead v. United States, a five vote majority held that the Fourth Amendment did not prevent warrantless wiretapping.56 Justice Brandeis, whose views ultimately prevailed, wrote in dissent that constitutions must be interpreted with technological advancements in mind in order to preserve fundamental rights.57 Eventually, the Court came to share Justice Brandeis' views, overruling Olmstead in Katz v. United States, 389 U.S. 347, 351 (1967). The Court applied Fourth Amendment requirements to electronic surveillance, reasoning that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." Id. at 352. The same understanding should be applied to the ability to encrypt speech.

3. Appellants Have Not Shown That The Publication of Cryptography Would Cause Direct, Immediate and Irreparable Harm to National Security

As demonstrated above, the cryptography regulations fail the Freedman analysis. In addition, however, the cryptography regulations must meet the substantive prior restraint requirements of New York Times Co. v. United States, 403 U.S. 713 (1971), by proving that publication would "surely result in direct, immediate and irreparable damage to our Nation and its people." Id. at 730 (Stewart, J. concurring). Here, the government asserts a strong national security interest in maintaining a system of prepublication review, but provides no proof in support of its assertion. Instead, it flatly states that "the national security claims in the Executive Order "require[] no elaboration." Appellants' Brief at 35. While it is indisputable that national security can be a compelling national interest and that the Executive Branch is given broad latitude in performing its duties in this area, the Supreme Court has made clear that national security or "the phrase 'war power' cannot be invoked as a talismanic

incantation"58 to support its policies, as the government is attempting to do in this case. New York Times is particularly relevant to the Appellants' assertion of a compelling interest here. In that case, Justices Douglas and Black flatly rejected the government's national security "mantra" in New York Times, noting that "[t]he word 'security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment." New York Times, 403 U.S. at 719 (Black, J., and Douglas, J., concurring). Justice Brennan also rejected the argument that publication "'could,' or 'might,' or 'may' prejudice the national interest in various ways." Id. at 725 (Brennan, J., concurring). Here the government's stated concern is that speech about cryptography "may be used" to harm national security. 15 C.F.R. Sect. 742.15. Appellants' seek to distinguish New York Times as a case in which the government sought to restrict "disfavored speech." Appellants' Brief at 38. That is not how the Supreme Court saw it. Several Justices were convinced that American lives would be lost due to publication. See New York Times, 403 U.S. at 717 (Black, J., and Douglas, J., concurring). There, the government sought to restrict speech based on its expected consequences - harm to the national security. Their argument here is the same.59 Here, the District Court correctly applied the "exacting standard" governing prior restraints under which the government's asserted need "to break foreign encryption and conduct adequate surveillance 'in furtherance of world peace and the security and foreign policy of the United States,' . . . [is] clearly insufficient without more." Bernstein II, 945 F. Supp. at 1288; Bernstein I, 922 F. Supp. at 1436; see, e.g., Bernstein III, ER 569. Importantly, the Government has given directly contrary testimony to its assertions here regarding its national security interest in preventing Internet publication. Admiral J. M. McConnell testified before Congress that, "[e]ncryption software distribution via Internet, bulletin board or modem does not undermine the effectiveness of encryption export controls."60 Furthermore, Appellants' key declarant, William P. Crowell, of the National Security Agency, last year informed the House Committee on the Judiciary that "serious users of security products don't obtain them from the Internet." AER 375. Such testimony leads to the conclusion that Appellants do not even believe their national security assertions here. The fact that this case involves export regulations does not diminish the government's burden of proof. In Bullfrog Films, Inc. v. Wick, 847 F.2d 502, 509-514 (9th Cir. 1988), this Court invalidated USIA regulations regarding the export of educational, scientific and cultural audio-visual materials as being facially inconsistent with the First Amendment, overly broad and vague. Contrary to the government's present reading of that case, Bullfrog Films found that "the First Amendment protects communications with foreign audiences to the same extent as communication within our borders," and held that an export restriction would be justified only where the government demonstrated "a clear and direct threat to national security." 847 F.2d at 509 n.9, 511-512. 61 The government's national security claim boils down to the simple assertion that the capacity to encrypt speech brings with it the capability to inflict harm. But such an assertion cannot justify a prior restraint. "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 Asso. 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). Even outside of prior

restraint analysis, direct advocacy of illegality or violence cannot be punished without proof that the speaker intended that the illegal acts occur and that it was likely, under the circumstances, to occur imminently. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969). Ultimately, Appellants' simply argue that publishing encryption software makes it easier or more likely that a foreign person will use encryption software to frustrate American surveillance. But even under Brandenburg's principles, which are less stringent than those applicable to prior restraints, the mere publication of encryption software must so imminently facilitate this harm that it equals causing it. "Capacity" not only ignores remoteness in time completely, it expressly allows prosecution of a person "[e]ven if the person . . . does not intend or expect that the software will be used for purposes contrary to this country's national security and foreign policy interests"62 See Appellants' Brief at 33 n.13. Yet it is settled law that speech cannot be punished unless both imminence and harmful intention are proven.63

B. THE EXPORT CONTROLS ON CRYPTOGRAPHIC SPEECH ARE INVALID EVEN UNDER THE REDUCED FIRST AMENDMENT SCRUTINY THE GOVERNMENT ADVOCATES

Even if the cryptography scheme is subject to a more lenient First Amendment standard as Appellants' claim, the government has failed to demonstrate that the rules are constitutional. To survive intermediate scrutiny, Appellants must demonstrate that the government's national security interest is real "and not conjectural,"64 that its policies actually serve the purported interest, and that the cryptography scheme does not impose too great a burden on protected speech. Here, the government's defense of the scheme fails on all counts.

1. The Cryptography Scheme Does Not Further the Government's Asserted Interest

The government must prove that the cryptography regulations "in fact alleviate [the asserted] harms in a direct and material way." Turner Broadcasting System, 512 U.S. at 644. However, when the government seeks to regulate speech, or even "conduct commonly associated with speech," it is well-established that this test is not met when the information subject to regulation is publicly available. See, e.g., Florida Star, 491 U.S. at 535 (no meaningful public interest served by rape-shield statute which restricted further publication of already public information.).65 Nordyke v. Santa Clara County, 110 F.3d 707 (9th Cir. 1997) (ban on commercial speech related to gun sales at county fair enjoined where restriction does not curtail advertising and sale of guns elsewhere in the county). This principle applies even where a prior restraint on national security grounds might otherwise be upheld. United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis.), reh'g denied, 486 F. Supp. 5 (W.D. Wis.), dismissed, 610 F.2d 819 (7th Cir. 1979) (injunction dissolved after subsequent publication of H-bomb material). Here, the public availability of information about cryptography undermines the government's ability to serve its asserted interest for two reasons.

a. The Printed Matter Exemption Undermines the Claim That the Cryptography Scheme Serves the Government's Interest

In claiming a lack of any intention to censor ideas, Appellants claim that Professor Bernstein can export paper publications on cryptography. Appellants' Brief at 29. In other words, Professor Bernstein needs a license to publish Snuffle.c on the Internet, but he does not need a license to send a thousand paper copies to foreign persons overseas. Viewed on its face, the exemption for print communication "diminish[es] the credibility of the government's rationale for restricting speech in the first place." Ladue v. Gilleo, 512 U.S. 43, 52 (1994). This exemption belies the claim that "encryption [software] poses unique and serious threats to national security," because under it, encryption remains "freely available" to "technologically sophisticated" foreigners; indeed, "[d]efendants conceded at oral argument that the effect of [this] dichotomy would be to make it more difficult only for the inept." Bernstein III, ER 568 and 560. ("the government conceded that in only a slighter greater length of time and with some greater technological skill, the regulation could be defeated"). Thus, the distinction upon which the government hangs its entire argument is not one of substance, but of marginal convenience in the ability of a recipient to use the information conveyed. See, e.g., Bernstein II, 945 F. Supp. at 1279 n.10. Appellants further demonstrate their unbridled discretion to censor cryptographic speech by their hedging of the print exception. They expressly "reserve the right to control scannable source code." 61 Fed. Reg. 68575. In doing so, the government has placed the academic community on notice that it has merely decided not to license books - yet. Appellants' reservation of the right to control printed materials is an especially powerful reason why the scheme "is so irrational and administratively unreliable that it may well serve to only exacerbate the potential for self-censorship." Bernstein III, ER 560.

b. Encryption Software Is Widely Available Abroad

Another problem in Appellants' claim of harm to national security is that encryption software is widely available abroad. A limitation on domestic publication cannot be justified when the same speech is available from foreign sources. ACLU, 929 F. Supp. at 848, 882-83. In the case of cryptography, Rep. Bob Goodlatte reported that more than 500 foreign encryption products and programs that exceed the limits of U.S. export controls are available internationally.66

2. The Regulations Restrict Too Much Speech

Under either strict or intermediate scrutiny, any government regulation must not "impos[e] an unnecessarily great restriction on speech." Reno, 117 S. Ct. at 2347 (citation and quotation marks omitted). Here, the cryptography scheme restricts too much speech because it is too imprecise. Cryptographers wish to publish and exchange scientific work, ranging from technical information to computer programs. Appellants' wish to prevent foreign persons who are targets of U.S. intelligence-gathering efforts from obtaining U.S. cryptography because it may hinder those efforts. Even were this not a futile exercise, this prepublication licensing scheme sweeps far too broadly to fit this narrow interest. For every foreign person who may be targeted for U.S. electronic surveillance, there must be thousands if not millions who will never be. That the cryptography scheme sweeps excessively is obvious. The cryptography scheme does not "punish the few who abuse

rights of speech after they break the law" but "throttle[s] them and all others beforehand." Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 559 (1975) (emphasis in original). The "widespread impact" of the cryptography licensing scheme "gives rise to far more serious concerns" than could any injunction targeted at a specific publication or even a particular speaker; "unlike an adverse action taken in response to actual speech, this [scheme] chills potential speech before it happens." United States v. National Treasury Employees Union, 513 U.S. 454, 468 (1995).

C. THE DISTRICT COURT JUDGMENT IS PROPER

1. The Declaratory Relief Granted Is Appropriate

The Government asserts that the declaratory relief sought and obtained below "is unduly broad even if the [District Court's] First Amendment reasoning is accepted." Appellants' Brief. at 44-45. Appellants advance two arguments in support of this contention: (1) the judgment should be rewritten to erase "object code" from the definitional controls on "encryption software" envisioned by the cryptography scheme; and (2) the court's invalidation of the cryptography controls on encryption and decryption software "and related devices" must be redrafted to clarify the intended reach of the court's judgment. Neither has merit. There can be no dispute that the District Court has the authority to enter declaratory judgment where it is appropriate to do so. Title 28 U.S.C. Sect. 2201. Appellants contest the authority of the District Court to enter declaratory judgment, and aver that the judgment declaring cryptography controls on "encryption software" unconstitutional as a prior restraint on speech is improper, because it necessarily "encompasses not only source code but also object code." Appellants' Brief at 45. For three reasons, however, Appellants' contention is in error. First, the key assertion underlying Appellants' position -- that object code is "nonexpressive" and therefore cannot be regarded as "speech" under the District Court's First Amendment analysis -- is nowhere supported in the record, and, indeed, is contradicted by the very authority cited.67 As this Court observed in Sega Enterprises, 977 F.3d at 1524, copyright protection for an original expressive work in the form of a computer program naturally "extends to the object code version of the program." Id., at 1520.68 By analogy, therefore, both source code and object code constitute protected expression for purposes of First Amendment analysis. Second, the Government urges this Court to invoke a variety of statutory constructions to invalidate the declaratory relief entered below. Among these is the suggestion that the Court excise "object code" from the regulatory control of "encryption software," which is specifically defined to "includ[e] source code, object code, applications software, or system software." 15 C.F.R. Sect. 772. This Court need not tarry in rejecting Appellants' invitation. Canons of statutory construction, "are not a license for the judiciary to rewrite the language enacted by the legislature." United States v. Monsanto, 491 U.S. 600, 611 (1989) (citation omitted). Here, the regulatory language is clear. The regulations do not differentiate between the categories of expression covered by the cryptography controls on "encryption software" and, indeed, crafted a regulatory scheme expressly designed to encompass all expressive components of such software. See 15 C.F.R. Sect. 772. Whatever force there might be to Appellants desire to excise specified categories of expression from regulatory control, the short answer is that the regulations were not

written that way. See, e.g., Monsanto, 491 U.S. at 611. Third, Appellants' alternative argument -- that the invalidation of the cryptography controls on encryption and decryption software "and related devices" requires modification to clarify the intended reach of the District Court declaratory judgment -- is equally specious. Obviously the scope of declaratory relief granted in a given case must be considered in context. While it is certainly true that the word "devices" is not a defined term under the cryptography regulations, the District Court's Opinion makes plain that the court's declaratory relief is directed not to commodities (defined as "[a]ny article, material, or supply except technology and software," (15 C.F.R. Sect. 772)) (emphasis added), but to "software," and more specifically "encryption and decryption software," and related technology. No further clarification is required. Lastly, Appellants argue that a judicial declaration invalidating 15 C.F.R. Sect. 744.9(a) as a prior restraint on speech is foreclosed by this Court's decision in United States v. Edler Industries, 579 F.2d 516 (9th Cir. 1978). However, Edler is distinguishable from this case. First, Edler did not present a facial challenge. Here, in contrast, even if a narrowing construction were available to provide a scienter defense to prosecution under the cryptography scheme, the regulations continue as a facial prior restraint scheme fostering self-censorship. Moreover, in Edler, the Court held that where the commodity at issue could be used in either military or non-military applications, one must know or have reason to know that technical data at issue is "significantly and directly related" to the military application to be subject to prosecution under the ITAR. Id. at 521. Here, in contrast, the cryptography controls under the EAR, by their terms, exclusively concern non-military applications. See 61 Fed. Reg. 68585 (to be codified as 15 C.F.R. Sect. 772). Edler is therefore of doubtful relevance to the constitutional infirmities presented by the current regulatory scheme. See also AER 273, OLC Memo. ("We do not believe that [Edler] resolves the First Amendment issues presented by the restrictions on the export of cryptographic ideas.") Third, Edler was fundamentally about the "conduct of assisting . . . enterprises . . . " Edler, 579 F.2d at 521. This court clearly understood that commercial arms traffic is one thing, while scientific exchange is another. Yet, 15 C.F.R. Sect. 744.9 clearly applies to purely academic "technical assistance." Accordingly, the District Court properly granted declaratory relief on these issues.

2. The Injunction Is Appropriately Tailored To The Circumstances Of This Case

Although Appellants do not separately address the issue, the scope of injunctive relief afforded below is appropriate for each of five reasons. First, as set forth above, Professor Bernstein established the merits of his case. The cryptography regulations plainly lack the required protections for prior restraints on speech and even fail the tests for content-neutral regulations proposed by Appellants. Second, Professor Bernstein continues to suffer an actual, not just threatened, violation of his First Amendment rights. As the U.S. Supreme Court has held, the "[l]oss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury" justifying injunctive relief. Elrod v. Burns, 427 U.S. 347, 373 (1976). Third, the finding the Professor Bernstein's First Amendment rights have been abridged, and will continue to be abridged, without the granting of injunctive relief leads to the conclusion that the

he has no adequate remedy at law. Professor Bernstein can never be made whole by an award of money damages. He instead seeks only what the Constitution commands: the right to write and publish his work and to receive such materials from others. Only an injunction preventing enforcement of the cryptography controls, and allowing Professor Bernstein to exercise his constitutional right to speak in the language and medium employed in his field of applied research, will make him whole. Fourth, the balance of equities favors Professor Bernstein. As noted above, he has suffered and will continue to suffer irreparable harm if the District Court's injunction is not upheld. In contrast, the only harm to Appellants if the injunction is upheld is the judicially noncognizable harm that will result from not being able to enforce unconstitutional regulations. Last, there is a peculiarly strong reason for upholding the nationwide relief afforded in this case. The First Amendment encompasses not only the right to speak, but the right to listen and exchange information. See Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 756 (1976) (where a speaker exists . . . the protection afforded [by the First Amendment] is to the communication, and to its source and to its recipients both") (emphasis added). Professor Bernstein wishes to publish, discuss and exchange his ideas with others in all public forums, including the new and unique public forum commonly known as the Internet. As demonstrated above, these types of academic discussions and exchanges are at the heart of the First Amendment as well as the scientific method, which requires that new ideas and their applications continually be tested and discussed in the marketplace of ideas. See supra at 35-71; Gordon & Breach Science Publishers S.A. v. American Institute of Physics, 859 F. Supp. 1521, 1541 (S.D.N.Y. 1994) (debate in academic journals is "near the core of the First Amendment"). Without the full injunctive relief afforded by the District Court, however, there will be no exchange -- Professor Bernstein could "speak," but no one may reply. In short, the First Amendment right of Professor Bernstein to listen, learn, discuss, explain, and otherwise "test" his work in the marketplace of ideas cannot be protected unless the rights of others to speak, discuss and engage in academic exchange are also protected. Accordingly, Professor Bernstein asks that the Court lift the stay pending appeal, and affirm the District Court's judgment for injunctive relief in its entirety.

VI. CONCLUSION

Appellants' argument here in a sense parallels that in Reno, where the government claimed a compelling interest in restricting children's access to indecent speech. That interest did not justify broad suppression of speech addressed to adults, however, because the government may not reduce adult speech to what is fit for children. Reno, 117 S. Ct. at 2346. That principle, paraphrased, is applicable here: A government agency may not be given unfettered discretion to reduce Americans' scientific speech, based upon its subject matter, to what is deemed fit for foreign targets of U.S. intelligence. Based upon the foregoing, Appellee respectfully requests that the District Court's decision be upheld in its entirety.

Dated: _____ McGLASHAN & SARRAIL
Professional Corporation

By:_____

FOOTNOTES

1 When this case began, Professor Bernstein was a Ph.D. candidate in mathematics at the University of California at Berkeley. He has since received his degree and has begun his academic career.

2 This action is a facial challenge to the government's regulations as they relate to encryption software, technology and technical assistance ("cryptography regulations"). Most of the cryptography regulations were promulgated by Appellants on December 30, 1996 and were inserted into the already existing Export Administrations Regulation (EAR), which operate pursuant to the authority granted in the Export Administration Act (EAA). See infra at 8-9. Specifically, this challenge extends to the restrictions which the regulations place on encryption software, controlled under ECCN 5D002, encryption technology, controlled under ECCN 5E002 and encryption-related technical assistance controlled by 15 C.F.R. Sect. 744.9. Plaintiff submits that on their face these three categories create an unconstitutional prior restraint on scientific speech.

3 National Research Council, Cryptography's Role in Securing the Information Society (1996) ("NRC Report").

4 The OLC found that the "requirement of a license as a prerequisite to exports of cryptographic information clearly raises First Amendment questions of prior restraint." Applying Supreme Court precedents, OLC identified "at least two fundamental flaws" in the export regime: (1) "the standards governing the issuance or denial of licenses is not sufficiently precise to guard against arbitrary and inconsistent administrative action," and (2) "there is no mechanism established to provide prompt judicial review" of licensing decisions. Memorandum of John M. Harmon, Assistant Attorney General, Office of Legal Counsel, to Dr. Frank Press, Science Advisor to the President (May 11, 1978). Appellee's Exceprts of Record ("AER") 240-55.

5 David Kahn, The Codebreakers: The Story of Secret Writing at 68 (1973, abridged version).

6 Talley v. California, 362 U.S. 60, 65 (1960).

7 Alan Pell Crawford, Founding Fathers' Forum, Wall Street Journal, Feb. 2, 1995 at A16.

8 Ralph E. Weber, Masked Dispatches: Cryptograms and Cryptology in American History 4 (Center for Cryptographic History, 1993).

9 In late 1981, the presidents of five major universities signed letters to Appellants that they were "deeply concerned about recent attempts to apply to universities the [export restrictions]". National Academy of Sciences, Scientific Comm. & National Security, 136-139 (1982).

10 See Allen M. Shinn, Jr., The First Amendment and the Export Laws:

Free Speech on Scientific and Technical Matters, 58 George Washington Law Review 368, 371 (January 1990). See also M. Christina Ramirez, The Balance of Interests Between National Security Controls and First Amendment Interests in Academic Freedom, 13 J.C. & U.L. 179, 192 & n.101 (Fall 1986).

11 The Government's Classification of Private Ideas: Hearings Before a Subcomm. of the House Comm. on Gov't Operations, 96th Cong. 2d Sess., H. Rep. No. 96 1540 (1980) at 67. Foreshadowing this case, the Report also noted that "efforts by the intelligence community to restrict public cryptography pose enormous questions of constitutional validity." Id at 63.

12 Appellants specifically noted that "neither [Professor Junger nor Mr. Miller] provided the software to the Government for any determination as to whether it was covered by the ITAR." AER 424. These examples demonstrate that the cryptography regulators act as prepublication censors of academic materials.

13 Senator Trent Lott, Cong. Rec. S10879-S10881 (October 21, 1997). See FBI Director Raises the Ante: Government Wants Mandatory Key Recovery, 2 Electronic Information Policy & Law Report 927, 930 (Sept. 12, 1997).

14 International Traffic in Arms Regulations, 22 C.F.R. Sect. 120.1-130.17 (1994), promulgated pursuant to the Arms Export Control Act 22 U.S.C. Sect. 2778.

15 922 F.Supp. 1426 (N.D. Cal. 1996).

16 As noted above, the cryptography regulations were inserted into the EAR, which implement the EAA. Because the EAA expired in 1994, the regulations are currently authorized by the International Emergency Economic Powers Act (IEEPA). Executive Order No. 13,026.

17 "Technology" is defined as the specific information necessary for the "development", "production", or "use" of a product. The information takes the form of "technical data" or "technical assistance. 15 C.F.R. Sect. 772.

18 Nuclear Pacific, Inc. v. United States Department of Commerce, No. C84 49R (W.D. Wa. June 8, 1984) (order denying motion to dismiss), see e.g. Milena Ship Management Co. v. Newcomb, 804 F. Supp. 846, 859 (E.D. La. 1992), aff'd, 995 F.2d 620 (5th Cir. 1993), cert denied, 510 U.S. 1071 (1994) (IEEPA does not bar judicial review of certain asset blocking actions by the Office of Foreign Assets Control).

19 15 C.F.R.ßß 732.2(b), (d), 734.3(b)(3), 734.4, 734.7(c), 734.8(a), 734.9 and Supplement No. 1 to Part 734, & 15 C.F.R. ß 768.1(b).

20 Another example of this absurdity is the regulatory treatment of a cryptographic algorithm called the Data Encryption Standard, or DES. The U.S. Government itself has written the specifications for DES software and has published them worldwide. As a result, DES is widely implemented into computer programs, is used all around the world and is available from many foreign Internet sites. Yet publication of DES source code on a U.S. Internet site still requires a license. NRC Report at 314.

21 An "algorithm" is the mathematical term for a set of instructions or recipe. Gottschalk v. Benson, 409 U.S. 63, 65 (1972) ("A procedure for solving a given type of mathematical problem is known as an algorithm.")

22 AER 6 & 7. Since he wrote Snuffle, Professor Bernstein has also written other cryptographic algorithms and expressed them as computer programs. AER 342-3. Under stipulation with the government, and subject to publication restrictions, he was permitted to teach some of them in a university course on cryptography in spring semester 1997. AER 484-489.

23 Eventually Professor Bernstein submitted a second round of five separate requests to the State Department, each of which asked if he could publish a different Snuffle-related item. AER 8-17. He divided his items up in order to give the Appellants the opportunity to consider each item separately. AER 13-14. On October 5, 1993 the State Department notified Professor Bernstein that all of the referenced items were defense articles under Category XIII(b)(1). Bernstein I, 922 F. Supp. at 1430 (emphasis in original). Believing that further appeal would be futile or ignored, he did not appeal Defendants' second determination.

24 The District Court specifically noted: "plaintiff had every reason to believe his paper had been determined to be a defense article until defendants' clarifying letter of June 29, 1995." Bernstein I, 922 F. Supp. at 1437 n.19.

25 The Instructions are controlled as "technology." See AER 42-44.

26 Defendants have even exercised their discretion beyond the plain language of their regulations. They have told several persons who wish to export software with no capability to encrypt that an export license is required merely because a recipient might later add encryption capability. See AER 81-3 and 502-6. The lack of judicial review makes it impossible to challenge such plainly improper regulatory applications.

27 Appellees agree that the constitutionality of the cryptography regulations is subject to de novo review by this Court. Appellants' Brief at 23.

28 The Government's claim regarding the neutrality of the EAR scheme as a whole is irrelevant. Both Plaintiff's challenge and the district court decision are limited to the regulations on cryptography which are significantly more restrictive than the EAR. See supra at 12-13.

29 Appellants' Brief at 27. See also ER 308 (Joint Statement). ("[c]ryptographic source code - cryptographic algorithms in a computer programming language such as 'C' - can be read and evaluated by computer scientists, mathematicians, programmers and others who possess the training or ability to understand such code").

30 See AER 431-2. See also Appellants' Brief at 33 n.13 (export controls apply "[e]ven if the person exporting the software does not intend or expect that the software will be used for purposes contrary to this country's national security and foreign policy interests").

31 Keyishian v. Board of Regents, 385 U.S. 589, 603 (1967). The Supreme Court has stressed that society has an interest in preserving "freedom of expression by the scientists and engineers," Bush v. Lucas, 462 U.S. 367, 371 (1983) and this Court has characterized scientific expression and debate as part of First Amendment "heartland." United States v. U.S. District Court, 858 F.2d 534, 542 (9th Cir. 1988).

32 Final Report of the National Commission on New Technological Uses of Copyrighted Works ("CONTU Report"), at 6 (July 31, 1978).

33 "[T]he Framers intended copyright itself to be the engine of free expression." Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 558 (1985). Copyright law expressly recognizes that computer programs are "literary works." 17 U.S.C. ßß 101, 117. See also Sega Enterprises Ltd v. Accolade, inc., 977 F.2d 1510, 1519 (9th Cir. 1993). Alfred C. Yen, A First Amendment Perspective on the Idea/Expression Dichotomy and Copyright in a Work's Total Concept and Feel, 38 Emory L.J. 393, 430, n.190 (1989).

34 Appellants propose a First Amendment exception for speech which can also be used to control a machine without necessarily conveying information to the user. Appellants' Brief at 27. But this exception could prove much more dangerous than it may appear. For example, computers can already understand sheet music, allowing, for example, a person who does not understand musical notation to nonetheless direct a computer to play a song. The government's proposal could mean that as computers become more adept at understanding human language, more forms of fully protected speech, such as sheet music, would become less protected.

35 61 Fed. Reg. 68575. Even when code is not published in scannable form, the government's purported distinction breaks down. See Bernstein II, 945 F. Supp. at 1279 n.10 ("They think terrorists can't type?"). On the basis of "capacity", the government could as easily "reserve the right" to restrict non-scannable source code, or even academic papers to the extent such materials could be used by foreign persons to develop encryption capability.

36 Mutual Film Corp. v. Industrial Com. of Ohio, 236 U.S. 230, 242 (1915).

37 Id. at 242, 244.

38 Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 502-03 (1952). See also United States v. Paramount Pictures, Inc., 334 U.S. 131, 166 (1948).

39 See New York v. Ferber, 458 U.S. 747 (1982); Freedman, 380 U.S. at 51.

40 See Appellants' Brief at 6 and citations therein.

41 The most well-known aspect of the Internet, the World Wide Web, was originally developed for physics research and only later "extended beyond the scientific and academic community." ACLU, 929 F. Supp. at 836 (finding 35); see id. at 831-832 (findings 5-14); id. at 834 (finding 48). See also AER 124-6; 73-6; 104-110; 65-9; 140-1; 183-6; 188.

42 AER 187-9; 74-5.

43 See Reno, 117 S. Ct. at 2335. ("There are thousands of [newsgroups], each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls.").

44 AER 16-7; 75; 174-5; 178.

45 AER 350-4.

46 For instance Professor Bernstein plans to consult Mr. Peter Gutmann, who Professor Bernstein believes lives in New Zealand. Mr. Gutmann has extensive experience in practical cryptography. AER 10.

47 Even if Professor Bernstein were not a teacher, however, his scientific publication may not be restrained. A person's right to participate in scientific discussion does not depend on his job title; Albert Einstein was a patent office clerk when he developed his theory of relativity.

48 117 S. Ct. at 2348. Compare Appellants' Brief at 36 ("the EAR's provisions regarding encryption technology 'leave ample alternative channels of communication' ").

49 Appellants correctly point out that the speech "at the center of this prior restraint claim is not the messages scrambled by encryption software, but rather encryption software itself." Appellants' Br. at 15 (emphasis in original). However, if the government sought to regulate the use of envelopes in the transmission of First Class mail, there would nevertheless be a First Amendment issue as to those correspondents who would use envelopes to secure the privacy of their letters. The ability to use encryption operates in the same way for electronic mail.

50 18 U.S.C. ß 798. See also 22 C.F.R. ß 121.01 ("speech scramblers").

51 Wooley v. Maynard, 430 U.S. 705, 714 (1977), quoting West Virginia State Board of Education v. Barnette, 319 U.S. 624, 637 (1943).

52 Barnette, 319 U.S. at 642.

53 E.g., Bartels v. State of Iowa, 262 U.S. 404 (1923); Meyer v. Nebraska, 262 U.S. 390 (1923). The foreign language prohibitions in Bartels and Meyer had been prompted by the hostilities with Germany in World War I. But the Meyer Court held that, despite the "[u]nfortunate experiences during the late war," the asserted state interest in domestic security could not justify encroachment on fundamental rights. 262 U.S. at 401-02.

54 McIntyre v. Ohio Elections Commission, 115 S. Ct. 1511, 1524 (1995); Talley v. State of California, 362 U.S. at 64.

55 Bates v. City of Little Rock, 361 U.S. 516 (1960); NAACP ex. rel Patterson v. State of Alabama, 357 U.S. 449 (1958). See also Lamont v.

Postmaster General, 381 U.S. 301 (1965).

56 277 U.S. 438, 464 (1928).

57 Foreshadowing the types of surveillance now possible in a computer based society, Justice Brandeis warned that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." He concluded that failure to extend constitutional protection to the novel question of wiretapping would mean that "[r]ights declared in words might be lost in reality." Id. at 473-74 (internal quotations omitted).

58 United States v. Robel, 389 U.S. 258, 263-64 (1967), quoting Home Bldg. & Loan Assn. v. Blaisdell, 290 U.S. 398, 426 (1934).

59 Indeed, the government in New York Times even asserted an interest much like that claimed here. It argued to the D.C. Circuit that suppression was necessary to preserve government secrets relating to cryptography, including the fact that the United States could decode North Vietnamese communications. See John Cary Sims, Triangulating the Boundaries of the Pentagon Papers, 2 Wm. & Mary Bill of Rights J. 341, 449 (1993).

60 Statement of Vice Admiral J. M. McConnell, Hearing on The Administration's Clipper Chip Key Escrow Encryption Program, S. Hrg. 103-1067, 103d Cong., 2d Sess. (May 3, 1994) at 155, attached as Exhibit B to Appellee's Opposition to Emergency Motion to Stay.

61 The government asserts that the First Amendment may not apply "with full force in this case" because of the "foreign locus of the EAR's export controls and the national concerns that underlie them." Appellants' Brief at 24 n.9, relying on Haig v. Agee, 453 U.S. 280 (1981). Haig involved the revocation of a passport of a former CIA employee whose actions resulted in episodes of violence and led to several deaths. 453 U.S. at 285 & n.7. The Supreme Court held that the revocation was consistent with Near v. Minnesota, 283 U.S. 697 (1931), which permits such actions to prevent "actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops."

62 Technical assistence requires mere "intent to assist in the development abroad" of cryptography. 15 C.F.R. Sect. 744.9(a).

63 See, e.g., Florida Star v. B.J.F., 491 U.S. 524, 539 (1989) (need for scienter requirement); NAACP v. Claiborne Hardware, 458 U.S. 886 (1982). Brandenburg has been applied to bar civil liability for speech that described dangerous or harmful acts. Herceg v. Hustler Magazine, 814 F.2d 1017 (5th Cir. 1987), cert. denied, 485 U.S. 959 (1988); Rice v. Paladin Enterprises, Inc., 940 F.Supp. 836 (D. Md.), appeal docketed, No 96 2412 (4th Cir. 1996).

64 Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 644 (1994) (citation omitted).

65 Further, the fact that Internet publishing is a form of mass

communication is not a proper basis for restricting it. Florida Star, 491 U.S. at 540-541 ("Where important First Amendment interests are at stake, the mass scope of disclosure is not an acceptable surrogate for injury.").

66 AER 362. See also GAO, Communications Privacy: Federal Policy and Actions, GAO/OSI-94-2, Nov. 4, 1993 at 27; Encryption Foreign Availability: How Much Evidence Do You Need? Export Control News, July 31, 1994 at 5; Declaration of David Balenson submitted as Exhibit G to Appellee's Opposition to Motion for Emergency Stay.

67 See Anthony L. Clapes, Confessions of an Amicus Curae: Technophobia, Law, and Creativity in the Digital Arts, 19 Dayton L. Rev. 903, 941 (1994) ("In the early days of programming, programs were written by humans directly in object code form. Object code could obviously be read in those days.").

68 ISC-Bunker Ramo Corp. v. Altech, Inc., 765 F. Supp. 1310, 1320 (N.D. Ill. 1990), also cited by Appellants, similarly holds that computer programs are "original works" entitled to federal copyright protection, making no distinction between source code and object code.