ROBERT D. McCALLUM Jr.
Assistant Attorney General

DAVID W. SHAPIRO
United States Attorney

JOCELYN BURTON
Assistant United States Attorney
California Bar No. 135879
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198

VINCENT M. GARVEY
Deputy Branch Director

ANTHONY J. COPPOLINO
Senior Trial Counsel
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470

Attorneys for the Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO HEADQUARTERS

DANIEL J. BERNSTEIN	C 95-0582 MHP
Plaintiff,	**DEFENDANTS' OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT.**
v.	
UNITED STATES DEPARTMENT OF COMMERCE et al.	Date: October 7, 2002 Time: 2:00 p.m. Courtroom: 15 [18th Floor] Chief Judge Marilyn Hall Patel
Defendants.	

Submitted: August 2, 2002

INTRODUCTION

Plaintiff's motion for summary judgment confirms the jurisdictional and substantive flaws with his Second Supplemental Complaint as set forth in defendants' motion to dismiss, or for summary judgment.[1]

First, plaintiff concedes that his claims about the Export Administration Regulations ("EAR") are based on his own "descriptions of the literal meaning of the EAR" and "are not meant as statements about the legal effect of the EAR." Declaration of Daniel J. Bernstein, ¶ 2. This presents fundamental jurisdictional concerns. See Defs. Mem. at 9-12. Plaintiff has ignored statements about the effect of the EAR on his activities made by the governing regulatory authority – the Department of Commerce – in its regulations and in three advisory opinions issued during a year of consultations permitted by the Court. Instead, he raises several theories based on his own "literal" reading of the EAR, without even referring to the Commerce Department's position on these issues.[2] The law is clear that allegations based on speculation, even as to constitutional injury, are insufficient to sustain standing. Laird v. Tatum, 408 U.S. 1, 13-14 (1972). Plaintiff is simply grasping for a continued dispute with the government in the face of significant regulatory changes and advice he has received.

Second, with the exception of two software programs attached as exhibits, plaintiff fails to submit the cryptographic software as to which he seeks broad injunctive relief, despite being forewarned that he has not ripened this aspect of his renewed complaint. This is a significant omission by Bernstein. Defendants have reviewed the two programs attached to Bernstein's declaration (SPRAY and DH224), and have obtained from public sources two other software programs at issue in his Second Supplemental Complaint (NISTP224 and HASH 127). None of these programs constitute software subject to encryption licensing controls under the EAR. See Second Declaration of Bernard Kritzer. Other programs mentioned in the Second Supplemental Complaint (MMERCT, RWB100, UIDwall) were never submitted to the government. As such, plaintiff is challenging encryption software regulations

[1] Hereafter "Pl. Mem." and "Defs. Mem." respectively.

[2] Indeed, plaintiff only submits one of the advisory opinions. See Tab G to the Declaration of Daniel J. Bernstein.

without having demonstrated that his software is subject to the EAR at all. See Defs. Mem. at 7-9.

Third, if the merits are reached, defendants reiterate the key point of our opening brief: whatever the Court's view of the prior encryption licensing requirements, this is now a very different case. In lieu of a general licensing requirement, the government now requires an email notice by the time encryption source code (and corresponding object code) is made publicly available (e.g. by posting to the Internet) or, if the exporter prefers, submission of a copy of the software. These EAR provisions do not regulate the content of ideas, but are focused on the export of software that provides a technical capability to encrypt, much like hardware. The regulations further the significant interest of providing the government some notice of what encryption it may encounter in the collection of crucial foreign intelligence, but do not restrict the widespread publication of academic or scientific information on cryptography. For these reasons, set forth further below, this case should now be dismissed.

PROCEDURAL HISTORY

Plaintiff's thirty line "procedural history" of the case contains several errors, and a significant omission. See Defs. Mem at 2-5. Plaintiff first states that this Court first held that his "censored documents were speech under the First Amendment." See Pl. Mem. at 2. Fairly stated, the Court held that encryption source code was protected expression, and that plaintiff had raised colorable claims in his first Complaint to withstand a Rule 12(b)(6) motion. See Bernstein v. Department of State, 922 F. Supp. 1426 (N.D. Cal. 1996). The Court did not rule that defendants had "censored" any "documents."[3]/

Next, plaintiff asserts that, after the State Department regulations initially at issue were enjoined by the Court's decision of December 9, 1996, see Bernstein v. Department of State, 945 F. Supp. 1279 (N.D. Cal. 1996), "the Commerce Department promptly issued new regulations." Pl. Mem. at 2. The regulations issued by the Commerce Department never purported to be a "response" to the Court's decision. In November 1996 – three weeks before the Court ruled – the President had announced that encryption export regulations would be transferred to the Commerce Department. See E.O. 13026, 61 Fed. Reg. 58767 (Nov. 19, 1996). The amendments to the EAR issued on December 30, 1996, maintained largely the same export licensing policy as in the ITAR. As such, the Court issued a decision

[3] Indeed, the Court specifically found that Bernstein's claims as to his "paper" were moot, and focused on licensing requirements on his source code. Bernstein, 922 F. Supp. at 1434.

concerning the EAR which superceded its prior order concerning the ITAR. See Bernstein v. Department of State, 974 F. Supp. 1288, 1310 (N.D. Cal. 1997). That decision, as to then-current regulations, was appealed.

Plaintiff next asserts that the "Ninth Circuit held that EAR was an unconstitutional prior restraint." Pl. Mem. at 3 (citing Bernstein v. Department of Justice et al., 176 F.3d 1132 (9th Cir. 1999)). This is the first of several instances in which plaintiff cites an appellate decision that no longer exists. See Pl. Mem. at 3, 23, 25. As should be obvious, no appellate decision concerning the validity of the prior regulatory regime was ever finalized. When the government's petition for rehearing was granted, the panel decision was withdrawn. Bernstein v. Department of Justice et al., 192 F.3d 1308 (9th Cir. 1999). After superceding regulations were issued, the appeal was remanded without running its course. Defendants obviously had the right to contest the panel decision further had the prior regulations remained in place. Yet plaintiff cites that decision as if it were circuit precedent – even closing his brief with an indented quote from it. Id. at 25.

By far the most significant error in plaintiff's "procedural background" is what it omits: any discussion of three advisory opinions issued by the defendants in this action. See Defs. Mem. at 5-6 and Declaration of Bernard Kritzer, Tabs 3, 4, 5. After granting the parties one year to engage in consultations about the revised EAR provisions on encryption, which led to three advisory opinions, plaintiff disregards this entire process and its results.

CURRENT REGULATORY FRAMEWORK

Plaintiff next sets forth a regulatory "framework" which underscores that his Second Supplemental Complaint is based on his own unsupported theories, not on how the governing authority applies its regulation. Plaintiff at least states correctly that there are two distinct sets of regulatory provisions at issue in this case: those concerning (i) encryption "software" and (ii) "technology" under the EAR. See Pl. Mem. at 3. Before defendants address plaintiff's allegations, some background on these provisions may be useful.

1. EAR Encryption Software Provisions

December 1996 Encryption Regulations: In December 1996, the EAR established license requirements for certain "Encryption Items" -- both hardware and software. See 15 C.F.R. § 742.15, 61

Fed. Reg. 68572, 68580 (December 30, 1996) (Tab 1 hereto). Along with numerous other items subject to export control, Encryption Items are listed on the Commerce Control List and given classification numbers (called "ECCNs"). See 15 C.F.R. Part 772 (defining ECCN) and Part 774 (ECCN 5A002 for encryption hardware; ECCN 5D002 for encryption software; ECCN 5E002 for encryption technology). Because encryption items "can be used to maintain the secrecy of information and thereby may be used by persons abroad to harm national security, foreign policy, and law enforcement interests," they are subject to export licensing requirements to determine, on a case-by-case basis, whether an export "is consistent with U.S. national security and foreign policy interests." 15 C.F.R. § 742.15(a)(1)(ii). While some exceptions to these license requirements existed in December 1996, they pertained primarily to "mass market" encryption items with limited key lengths, and to "recoverable" encryption products. See 61 Fed. Reg. at 68581 (Dec. 30. 1996) (amending 15 C.F.R. § 742.15(b)(1), (2), (3)).

January 2000 Encryption Revisions: In January 2000, far broader exceptions to encryption license requirements were established for all encryption items, including software and hardware, as set forth in 15 C.F.R. Part 740. See 65 Fed. Reg. 2492-2502 (Jan. 14, 2000) (Tab 2 hereto). In particular, a license exception (called "TSU") was expanded for "unrestricted" encryption source code. Under this exception, encryption source code that would be considered publicly available was excepted from encryption export licensing requirements if they were not commercial items.[4]/ See 15 C.F.R. § 740.13(e), 65 Fed. Reg. at 2497. This license exception was directed at "open source" encryption items – that is, encryption source code made publicly and freely available on the Internet for downloading. See 65 Fed. Reg. at 2492.[5]/

On its face, the expanded license exception for software that would be considered publicly available eliminated requirements that were at the heart of plaintiff's prior claims – specifically, that a

[4]/ In the parlance of the EAR, this exception initially applied to software that was "not subject to an express agreement for payment of a licensing fee or royalty for commercial production or sale of any product using the source code." See 15 C.F.R. § 740.13(e), 65 Fed. Reg. at 2497.

[5]/ In October 2000, the EAR encryption provisions were further amended. See 65 Fed. Reg. 62600 (Oct. 19, 2000) (Tab 3 hereto). Among these revisions, corresponding object code compiled from encryption source code, that would also be considered publicly available, was given identical treatment in license exceptions. See 65 Fed. Reg. at 62605-06 (amending 15 C.F.R. § 740.13(e) and 740.17(b)(4)(i)).

license be obtained before Bernstein could freely make his encryption source code available to students, fellow academics, and the world at large on an Internet Web site or newsgroup. Bernstein's claim that, without a license, he could not "publish" his scientific papers containing encryption source code to the Internet no longer exists. The remaining requirement for such exports is that notice be provided by the time of export, either through an email identifying the particular Web site where the software is located, or by providing a copy of the software. See 15 C.F.R. § 740.13(e)(1); 65 Fed Reg. at 2497 (Jan. 14, 2000). In addition, although exports of encryption software to certain terrorist designated states remained prohibited, the revised EAR made clear that mere posting to the Internet does not constitute knowledge of such a prohibited export. Id. § 740.13(e)(3), 65 Fed. Reg. at 2497 (Jan. 14, 2000).[6]/

June 2002 Encryption Revisions: Most recently, on June 6, 2002, the Commerce Department issued a further revision to the regulations which made them even simpler by eliminating the distinction between license exceptions based on whether the source code (and corresponding object code) is linked to commercial development. See 67 Fed. Reg. 38855, 38862 (June 6, 2002) (Tab 4 hereto). Now, all encryption source code that would be considered publicly available (and corresponding object code) may be exported under the "unrestricted" license exception (TSU) regardless of whether it is subject to an express "commercial" agreement (i.e., for payment of a licensing fee or royalty for commercial production or sale of any product using the source code). For purposes of this lawsuit, dropping the distinction based on commercial development was not particularly significant, since both publicly available "commercial" and "unrestricted" encryption source code (and corresponding object code) were subject to similar license exceptions (TSU and ENC) under which only notice was required for their

[6] Indeed, under the January 2000 regulations, even *commercial* encryption source code that would be considered publicly available was excepted from general license requirements. See 65 Fed. Reg. at 2498 (amending 15 C.F.R. § 740.17(a)(5)(i) (License Exception ENC) (later at 15 C.F.R. § 740.17(b)(4)(i)), see 65 Fed. Reg. 62600, 62606 (Oct. 19, 2000). Other license exception provisions were expanded in January 2000 for exports of certain encryption items to U.S. subsidiaries, for exports to non-government end-users, and for certain "retail" encryption commodities and software. See 65 Fed. Reg. 2497-99 (Jan. 14, 2000) (amending 15 C.F.R. § 740.17(a)(1), (2), (3) (later at 15 C.F.R. § 740.17(b)(1), (2), (3), see 65 Fed. Reg. at 62605 (Oct. 19, 2000)). In addition, even most non-publicly available encryption source code could be exported, after a classification review, under the commercial license exception ENC to non-government end-users. See 65 Fed. Reg. at 2498 (Jan. 14, 2000) (amending 15 C.F.R. § 740.17(a)(5)(ii)) (later at 15 C.F.R. § 740.17(b)(4)(ii), see 65 Fed. Reg. at 62606) (Oct. 19, 2000).

export. The June 6 revision simply put all publicly available source code and corresponding object code into one regulatory category (License Exception TSU). The impact of the revised EAR on this case is the same as with the January 2000 provisions: there is no license requirement on plaintiff for posting encryption software publicly to his Internet Web site or a newsgroup.

2. Encryption Technology Provisions

Perhaps because license requirements on encryption source code were relaxed, plaintiff's motion shifts emphasis to alleged restrictions on academic activities under the EAR provisions on "technology." Unlike the encryption software provisions, the EAR "technology" provisions have remained fairly constant, and this aspect of plaintiff's "supplemental" complaint presents nothing "new" for adjudication.

By way of background, in addition to regulating the export of specific products (like encryption hardware and software), the EAR also regulates the export of information falling within the definition of technology, i.e., "specific information necessary for the 'development,' 'production,' and 'use' of a product," which may take the form of technical data or technical assistance. See 15 C.F.R. Part 772 (definition of technology). Courts have long recognized that export controls may legitimately include the regulation of technology and technical assistance. See United States v. Edler Industries, 579 F.2d 516, 522 (9th Cir. 1978); United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989); United States v. Van Hee, 531 F.2d 352 (6th Cir. 1976). The technology provisions of the EAR are solicitous of First Amendment activities by excluding information that is or will be made publicly available, publications, educational information, fundamental research, and academic discussion. See 15 C.F.R. §§ 734.7, 734.8, 734.9, 744.9.

ARGUMENT

I. THE EAR DOES NOT IMPOSE THE RESTRICTIONS ALLEGED BY PLAINTIFF.

Plaintiff's motion presents a series of meritless allegations that the EAR "prohibits collaboration at scientific conferences," requires notice for "private email" and "Web publications," and requires a license for "answering questions" and posting software to an Internet newsgroup, and even for exporting published books on encryption. See Pl. Mem. at 13. Each allegation is addressed in turn.

A. Collaboration at Conferences

Plaintiff first argues that the EAR provision concerning technical assistance on encryption, see 15

C.F.R. § 744.9, prohibits "collaborations involving EI software at scientific conferences." Pl. Mem. at 5. This contention is meritless. Plaintiff concedes that, under Section 744.9, there is *no* regulation of technical assistance in connection with publicly available encryption software exported under License Exception TSU. He argues, however, that this exception is effectively unavailable because it can be difficult to locate a telephone line for a laptop computer in order to email notice of an encryption software export. See Pl. Mem. at 6, 7. This scenario is detached from the regulations.

First, even apart from the exemption from technical assistance in Section 744.9, the EAR otherwise excludes publicly available information from the definition of "technology" – including information exchanged at an open, public conference. See 15 C.F.R. § 734.7(a)(4). Indeed, Bernstein concedes that publicly available "technology" (which is a term defined to include "technical assistance") is not subject to the EAR. See Pl. Mem. at 11. Also, Section 744.9 itself excludes the kinds of exchanges that occur at scientific conferences -- teaching, academic discussion, and the work of groups or bodies engaged in the development of standards -- from the reach of that provision. See 15 C.F.R. § 744.9. From these two provisions, it should be apparent that the EAR does not seek to regulate discourse at open, public scientific conferences, and they have not been so applied to plaintiff.

Beyond this, Section 744.9, as noted, further excludes from regulation any technical assistance concerning encryption that is subject to a license exception, e.g., publicly available encryption software. As such, plaintiff was advised that notice was *not* required should he develop publicly available encryption software outside of the United States. See Third Advisory Opinion, Tab 5 to Kritzer Declaration, at 3, ¶ (3). If, as part of that process, plaintiff exported encryption software from the United States, notice of an Internet posting or a copy of the software would be required. Id. In any event, it is meritless for plaintiff to elevate (a dubious) concern over the lack of a telephone line into a "prohibition" on scientific collaboration at conferences.

Plaintiff cites other provisions of the EAR which he claims impose the same restrictions. The "General Prohibitions" against "re-exports" that plaintiff cites, see Pl. Mem. at 6, on their face apply to "exports subject to the scope of the EAR." See 15 C.F.R. 736.2(b). Transfers of technology to a foreign person outside of the United States through oral communication would not apply to information that is not subject to the EAR to begin with, such as information exchanged at open, public conferences or academic discussions. Also, where the export qualifies for a License Exception under Part 740, it is not restricted by the General Prohibitions. Id.[7]

Finally, Bernstein also alleges that he cannot collaborate with colleagues at an overseas conference because the general requirement of knowledge for an EAR violation, see 15 C.F.R. § 764.2(e), makes him "vicariously liable" for the "predictable" actions of his foreign colleagues who may take software or technology home with them. See Pl. Mem. at 7-8. This, again, is unfounded. If academic discussion of cryptography at an open, public conference is at issue, the technology and technical assistance provisions of the EAR would not apply to plaintiff or his foreign colleagues, directly or vicariously.

B. Notification for Private Email

Plaintiff also claims that the EAR regulates "private discussions" in emails related to encryption information. See Pl. Mem. at 8. This argument is likewise without foundation. Plaintiff's theory is that, under the new license exceptions, "to release information from 'EI' controls requires disclosing the information to the government, either indirectly as an 'Internet location' or directly as 'a copy.'" See Pl. Mem. at 8. This argument distorts the regulations. The notice requirement at issue concerns the export of software, and does not extend to "private discussion" about cryptography contained in an email.[8]

C. Notification for "Web Publications"

Plaintiff next asserts that, to comply with the notice requirement for exports of encryption to the World Wide Web, he would have to "review all of his desired publications" and "every change to his Web changes" and make as many as three thousand notices per year to comply with the EAR. See Pl. Mem. at 10. This is specious. Bernstein raised this very scenario with the government during the consultation period and was specifically advised that the notice requirement would apply to changes in software where a new encryption algorithm is utilized in the source code whereby an identical input

[7] For the same reasons, Bernstein's assertion that Section 744.9 and Section 736.2(b)(1) prohibits him from "answering questions" on an Internet newsgroup, see Pl. Mem. at 11, is wrong.

[8] Bernstein's September 29, 2001, notification of the Internet location of NISTP224, which contains only a subject line URL and no text in the body of the email, suggests that he understands that the notice requirement does not extend to the content of private communications. See Tab D to Bernstein Declaration.

results in a different output. See Third Advisory Opinion, Tab 5 to Kritzer Declaration, at 2 n.3. This is very much a bright line standard. The government told Bernstein that it did not want thousands of notices -- just notice of new encryption programs based on new or different algorithms.

Bernstein's further claim that he does not understand when notice is required for encryption software exports because he cannot tell the difference between encryption that functions to maintain the confidentiality of text rather than merely to "authenticate" or protect a transaction, see Pl. Mem. at 9, is also meritless. Plaintiff has previously tried to build a constitutional claim on this thin-reed of an argument. From the beginning of this case, Bernstein has tried to "prove the point" that algorithms designed "to protect messages against forgery" (i.e. authentication programs) can also be used in software programs that "protect against eavesdropping" (i.e. provide data confidentiality). See Bernstein Decl. ¶ 90. Seven years ago, in a 1995 declaration, defendants explained that the regulations, including the ITAR, focused on encryption software that actually functions to scramble text, but not software that is limited to authenticating the security of a particular transaction, like a bank ATM transaction. See (First) Declaration of Louis F. Giles III ¶¶ 7, 8 (dated August 15, 1995) (Docket No. 18) (hereafter "(First) Giles Decl."). Bernstein's original Snuffle software utilized an "authentication" algorithm (called a hash function) in a program that functioned to maintain data confidentiality. See (First) Giles Decl. ¶ 18. The defendants explained that if the program functioned to maintain data confidentiality, it was subject to regulation. See (First) Giles Decl. ¶ 17.

This distinction is clear in the regulations, as well as technically. The EAR states that "Encryption Items" are those which "can be used to maintain the secrecy of information." See 15 C.F.R. 742.15. The applicable Commerce Control List entries for software and hardware that are subject to encryption license controls (ECCN 5D002 and 5A002) expressly exclude items limited to "authentication" – which is defined to include "all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorized access." See ECCN 5A002 (Technical Note 2). It should be obvious, even to a layperson, that software which functions solely to protect PIN numbers or passwords, in order to prevent tampering with a transaction, is different from software that functions to scramble plaintext. It should also be obvious that these different functions have far different national security implications. Bernstein himself sees the distinction between programs that provide "protection against forgery" and those which provide "protection against both forgery and eavesdropping." See Bernstein Decl. ¶¶ 84, 90, 107. For plaintiff to re-plow this ground seven years later is meritless.

D. Licensing for Assembly Language Programs

Bernstein next alleges that the EAR is constitutionally flawed because it supposedly continues to require export licenses for encryption software written in so-called "assembly languages" which, he argues, is not "compiled" software and, therefore, neither "encryption source code" nor "encryption object code" under the EAR. See Pl. Mem. at 10-11. Bernstein's says he "fears that the government would attempt to prosecute him" for exporting a program in "assembly language." See Pl. Mem. at 11. The Commerce Department has never indicated to Bernstein that assembly language programs would not benefit from the new license exception. See Second Declaration of Bernard Kritzer, ¶ 10. The various definitions of software in the EAR easily encompass different *types* of computer "programs" such as assembly language programs. Id.[9]/ This is yet another claim founded on Bernstein's own conjecture.

E. Licensing for Postings to Sci.Crypt

Perhaps Bernstein's most egregious assertion is that a license is required to post software to the Internet newsgroup Sci.Crypt because it may be downloaded in Iran or other terrorist nation, and Bernstein "knows" that these postings are available in Iran. The EAR addresses this explicitly and indicates that such postings to the Internet do not constitute knowledge of an impermissible export. See 15 C.F.R. § 740.13(e)(6) (as amended by 67 Fed. Reg. at 38862 (June 6, 2002)). The advisory opinions to Bernstein also explicitly address this. See First Advisory Opinion, Tab 3 to Kritzer Declaration at 1. Bernstein's assertion that a license is still required for such postings, without advising the Court of the regulations or advisory opinions, lacks a good faith basis.

[9] In 15 C.F.R. Part 772, the EAR defines: (a) "software" to mean "[a] collection of one or more 'programs' or 'microprograms' fixed in any tangible medium of expression; (b) "source code (or source language)" to mean "[a] convenient expression of one or more processes that may be turned by a programming system into equipment executable form ('object code' (or object language)); (c) "encryption software" to mean "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems" which "includes source code, object code, applications software, or systems software."; (d) "encryption source code" to mean "[a] precise set of operating instructions to a computer that, when compiled, allows for the execution of an encryption function on a computer."

F. License for Scientific Journals

Bernstein's final claim is that the EAR requires a license for scientific journals on the Internet. See Pl. Mem. at 12. Plaintiff twists the regulatory definition of "published" information to suggest that "[b]ooks, journals, and other items published by publishing houses . . . do not qualify as 'published' under the EAR." Id. This claim is frivolous. The EAR provides that "published information and software" that is *not* subject to export regulation includes "publication in periodicals, books, print, electronic, or any other media available for distribution to any member of the public or to a community of persons interested in the subject matter, such as those in a scientific or engineering discipline, either free or at a price that does not exceed the cost of reproduction and distribution." 15 C.F.R. § 734.7 (a)(1) (emphasis added). Bernstein distorts the last phrase in the provision, arguing that certain specified "costs" of publishing a book do not fall within the "cost of reproduction and distribution" and, hence, that published books are not exempt from the EAR. See Pl. Mem. at 12.[10]/

It should be emphasized, again, that this is another claim based on Bernstein's own reading of the EAR, and not on any effort by the government to restrict him from publishing a book. The very regulatory Supplement that Bernstein cites explains the purpose of the "cost of reproduction and distribution" phrase. In one example, the Supplement states – specifically with reference to the sale of *software* – that "reproduction and distribution costs may include variable and fixed allocations of overhead and normal profit for the reproduction and distribution functions" either in a company or for a third party distribution system. See 15 C.F.R. § 734, Supplement No. 1, Question G(2)(emphasis added). This covers the types of costs to which Bernstein alludes.

In another example, the Supplement to Part 734 states that if a manufacturer prepares "detailed handbooks and reference manuals on key aspects of the design and manufacturing processes" of an item subject to the EAR, and for which the cost of publishing such manuals is typically $500, but sets the sales price at $15,000, then the manual is not considered "publicly available." See 15 C.F.R. § 734, Supplement No. 1, Question A(5). This example merely explains the hardly exceptional notion that the

[10]/ He includes in such unspecified costs "author compensation, acquisition costs, editorial costs, illustration costs, design costs, typesetting costs, promotion costs, and profit." Id

"cost of reproduction" caveat to the public availability provisions cannot be used when the sales price of an item (in this example, a manual) is clearly beyond any conceivable cost of publishing (in this case, 30 times the "typical cost").[11]/ Bernstein's suggestion that the EAR seeks to preclude the export of publicly available "books, journals, and other items published by publishing houses," see Pl. Mem. at 12, is entirely unfounded.

II. PLAINTIFF'S SECOND SUPPLEMENTAL COMPLAINT DOES NOT PRESENT A JUSTICIABLE CASE OR CONTROVERSY.

Defendants reiterate that plaintiff's Second Supplemental Complaint does not present a justiciable case of controversy, for two reasons. See Defs. Mem. at 7-12 and 22.

Encryption Software: First, none of the software programs identified for the first time in the Second Supplemental Complaint were submitted to the Commerce Department for a classification review to determine if they are even subject to the EAR, and none of the four programs the government has reviewed (SPRAY, DH224, NISTP224, HASH 127) are "Encryption Items" under ECCN 5D002. See Second Declaration of Bernard Kritzer. Indeed, because these programs have been made publicly available, they are not even subject to the EAR. See Second Kritzer Decl. ¶¶ 6-9. The Court should not rule as to regulatory provisions on encryption software absent a demonstration that the software programs plaintiff places at issue are subject to them. See also Defs. Mem. at 7-9.

Academic Activities: Second, claims based on speculation, as detailed above, and not specific administrative determinations or threatened enforcement, are insufficient to establish standing. See Defs. Mem. at 9-12 and 22. It is apparent from plaintiff's motion that he challenges numerous EAR provisions as restricting his academic activities based solely on his own conjecture. See Section I, supra. This is an insufficient basis on which the Court may exercise jurisdiction.

[11]/ Also, even if priced higher than the cost of production and distribution, the export or reexport of technology or software in a library accessible to the public is not subject to the EAR. See 15 C.F.R. § 734, Supplement No. 1, Question A(5) and § 734.7(a).

III. THE EAR PROVISIONS ON ENCRYPTION SOFTWARE AND TECHNOLOGY ARE CONSTITUTIONAL.

To the extent the Court reaches the merits, defendants have set forth the constitutional analysis applicable to the EAR provisions on encryption software and technology. See Defs. Mem. at 12-25. After setting forth his regulatory analysis, Bernstein cites various authority at length, but does not demonstrate it is applicable here. Defendants address plaintiff's contentions in turn.

A. Encryption Source Code Has Both Expressive and Functional Qualities.

Bernstein begins his argument by reiterating that source code is "speech" for purposes of the First Amendment. Pl. Mem. at 13. This hardly begins the applicable analysis. The mere fact that something is expressive says nothing as to whether its regulation is somehow constitutionally impermissible, or even what standard of review applies to the challenged regulation. Throughout this case, Bernstein has conceded that source code is more than expressive -- that it can also be used to program a computer to perform a technical function to encrypt.

First, the parties stipulated that "'[c]ryptographic 'source code' is a computer program written in a computer language such as the 'C' language that can be used to encrypt and decrypt information" on a computer. See Joint Statement of Facts ¶ 6 (emphasis added).[12] The parties also stipulated that "[i]nformation sent via computers is, in the absence of cryptography, unsecure in transmission and may be viewed by those other than the intended recipient," but that "[w]ith cryptographic software, messages or text can be secured with the intention that whatever is sent is inaccessible to anyone except the intended recipient (who possesses the key)." Id. ¶ 5 (emphasis added). Plaintiff's own declarant admits that the "aim of encryption [is] to turn an otherwise intelligible message into gibberish, so that a person who intercepts the message cannot read it." (First) Declaration of Bruce Schneier. ¶ 2 (dated 7/26/96) (Docket No. 52) (emphasis added).[13]

[12] The Joint Statement of Facts was originally filed, in connection with prior cross-motions, on September 11, 1996 (Docket No. 75) and resubmitted on April 25, 1997 (Docket No. 127).

[13] See (Third) Giles Decl. ¶ 9 (4/29/02) (an encryption "source code" is a computer program that implements a cryptographic "algorithm" on a computer through the use of a computer programming language) and ¶ 8 (a cryptographic algorithm is a mathematical function or equation that can be implemented

Plaintiff himself described the functional capacity of his "Snuffle 5.0" software, stating it allows individuals to exchange encrypted text with "zero-delay," meaning that "Snuffle can be used for interactive conversations: each character typed by one person can be encrypted, sent to the other person, and decrypted by the other person immediately." See Plaintiff's First Commodity Jurisdiction Request to the State Department, Tab 3 to the Second Declaration of William Lowell (dated 7/26/96) (Docket No. 44). Plaintiff further described Snuffle software (snuffle.c and unsnuffle.c) as the items "which actually perform encryption and decryption." Id. (emphasis added). He also stated that Snuffle has a "practical use . . . for the purpose of interactively exchanging encrypted text." Id. (emphasis added). Finally, the parties stipulated that the steps necessary to encrypt data on a computer using source code are trivial.

> Compiling software performs the compiling function and is commonly available at retail computer outlets. With such software loaded, source code can be compiled into object code with the press of a button on a computer.

See Joint Statement of Facts ¶ 7 (emphasis added).[14]/

In its first opinion in this case, this Court characterized plaintiff's contention that source code, even as written on paper, should not be considered functional to any extent as "specious" – specifically noting "the ease with which one can convert source code into object code." See Bernstein v. U.S. Department of State, 922 F. Supp. at 1434, n. 14. Other courts have recognized that a computer software program is a set of instructions to a computer that directs computer hardware to perform certain tasks. See Universal City Studios v. Corley, 273 F.3d 429, 449-53 (2d Cir. 2001)("computer code can instantly cause a computer to accomplish tasks"); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1537 n.11 (11th Cir. 1996) and Digidyne Corp. v. Data General Corp., 734 F.2d 1336, 1342 (9th Cir. 1984), cert. denied, 473 U.S. 908 (1985) (software is "a set of instructions [to a computer] that allows the system to accomplish a particular task"). See also Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514 n.2 (9th Cir. 1993) and Johnson Controls, Inc. v. Phoenix Control Systems, Inc., 886 F.2d 1173, 1175

electronically in software to transform data into an unintelligible form).

[14]/ In addition, not all source code needs to be "compiled" for execution. For example, "interpreted programs can be executed "on the fly" – underscoring that source code is not merely an "informational" version of software. See (Third) Giles Decl. ¶ 10 (dated 4/29/02).

n.2 (9th Cir. 1989) ("source code" is a set of instructions to the computer, in programming languages such as BASIC or FORTRAN, and "object code" is the same set of instructions in binary code).[15] Moreover, in source code form, software can more easily be modified to perform different or additional functions, and is also more "portable" for use on different operating systems or for insertion into another program, such as a Web Browser. See (Third) Giles Decl. ¶ 11. In sum, even if expressive to some, source code unquestionably has functional qualities as well. It is the functional quality of source code that distinguishes it from newspapers or scientific "papers," and this affects the constitutional analysis, starting with the appropriate standard of review. See Universal City Studios, 273 F.3d at 449-452 ("functionality of computer code properly affects the scope of its First Amendment protection").

B. The EAR Provisions on Encryption Are Not Content Based.

In this round of motions, plaintiff emphasizes a different constitutional theory -- namely, that the export regulations at issue are directed at the content of speech. In so doing, plaintiff has (finally) identified the right constitutional question, but answers it incorrectly. The key inquiry in this case is whether the text and purpose of the EAR provisions on encryption software are directed at the content of ideas. As defendants have set forth, the answer is 'no' -- the EAR provisions at issue are content-neutral, and intermediate First Amendment review applies to them. See Defs. Mem. at 17-22. Bernstein argues that the EAR is content based because "it selects a specific type of information for control" -- namely "software" and, more specifically, software concerning "cryptography." See Pl. Mem. at 15. He argues that "[c]hecking whether a document contains strong cryptographic non-authentication computer-comprehensible instructions means engaging in a detailed inspection of content." Id. Finally, he argues that the EAR is content-based because it regulates what Bernstein calls "instructions" and "documents [that] contain instructions" that people can use to maintain the secrecy of information on computers. Id.

The fundamental flaw with this argument is that the regulation of software that, as Bernstein concedes, causes a computer to perform a technical function is not the regulation of the content of

[15]/ Circuit Judge Nelson's dissent underscores that the withdrawn panel decision failed to appreciate the functional quality of software in its First Amendment analysis. See Bernstein v. Department of Justice et al., supra, 176 F.3d at 1147-1150 (recognizing the "basic function of encryption source code to act as a method of controlling computers").

particular ideas. Resorting to argument by semantics, Bernstein labels a software program as a "document" which contains "instructions." Id. at 15. But he concedes that encryption software constitutes "*computer comprehensible* instructions" which can be used to maintain the secrecy of information on a computer. Id. That has been defendants' point throughout the case. The regulation of software programs that direct a computer to conceal data is not a regulation of mere "ideas" inherent in the program but, rather, of an item that performs a technical function. This simple point -- that source code, while expressive to some, also performs a technical function -- cannot credibly be disputed.[16]/

Moreover, the text of the EAR pertains to all encryption products -- hardware and software -- which are included among other commodities on the Commerce Control List whose export is regulated for national security or foreign policy reasons. See 15 C.F.R. Part 774. The regulations state specifically that encryption hardware and software are subject to the EAR because of their functional capacity to maintain the secrecy of information on a computer. See 15 C.F.R. § 742.15. The concern is with the spread of an encryption function, not the publication of ideas and information about encryption which, as defendants have previously shown, are broadly published in the United States and overseas.[17]/ Cryptographic algorithms and theories are widely published. The Data Encryption Standard was published by the government. See Federal Information Processing Standards Publican 46 (January 15, 1977) (Tab 10 to Crowell Declaration). Academic journals abound with details of mathematical encryption theories. Numerous textbooks explain cryptographic theories. Academic conferences on cryptography are a regular occurrence. The EAR is not directed at controlling the publication of academic or scientific ideas concerning cryptography, but at the capability to implement encryption

[16]/ Nor can source code accurately be compared to a "chocolate chip cookie recipe." See Pl. Mem. at 16. Computer source codes are not instructions which inform people how to mix ingredients; they are instructions to a microprocessor which cause a computer to function a certain way, in this case to encrypt data or text being transmitted through a computer.

[17]/ Examples of scientific articles, textbooks, and open conferences on cryptography, as well as academic courses, have been placed in evidence previously. See Second Declaration of Louis F. Giles III, ¶¶ 1-5 and Tabs 1-5 (dated 10/5/95) (Docket No. 31); Declaration of William P. Crowell, ¶¶ 23-32 and Tabs 1-10 (dated 7/26/96) (Docket No. 95); Declaration of Anthony Coppolino, ¶¶ 3-9 and Tabs 1-3, 6-7 (dated 8/30/96) (Docket No. 73) and Second Declaration of Anthony Coppolino, ¶¶ 2-3 and Tabs 1-25 (dated 10/18/96) (Docket No. 95).

functions in hardware and software. By contrast, in cases where the Supreme Court has found laws to be content-based, it is apparent that specific substantive ideas are being targeted.[18] None of this authority pertains to export requirements on encryption products, including encryption software programs.

C. The EAR Provisions on Encryption Satisfy Intermediate Scrutiny.

In our opening memorandum, defendants set forth the application of the intermediate review standard to the EAR provisions at issue. See Defs. Mem. at 20-22. In response to plaintiff's motion, one issue must be addressed. Plaintiff argues that the success of prior terrorist attacks against the United States somehow negates the government's interest in taking steps to prevent such attacks. See Pl. Mem. at 1.[19] Plaintiff is in no position to assess the government's national security interests and how they should be met. Those interests are substantial on their face. Encryption products can unquestionably be used to conceal information. See (Third) Giles Declaration ¶ 5 (dated 4/29/02). In the wrong hands, such items have unquestioned national security implications. Id. ¶¶ 6-7. Notice or a copy of which such software is leaving the country provides a valuable head-start in preparing to deal with encryption that has fallen into the hands of a hostile adversary. Id. ¶¶ 16-17. Courts have recognized that the decision on the extent to which a particular commodity should be regulated for export inherently involves national security and foreign policy judgments.[20] The threat to national security posed by terrorism,

[18] See City of Cincinnati v. Discovery Network, 507 U.S. 410 (1993) (ordinance barring distribution of "commercial" advertising content-based); Linmark Associates v. Township of Willingboro, 431 U.S. 85 (1977) (ordinance forbidding use of specific content -- "For Sale" and "Sold" signs – content based); Burson v. Freeman, 504 U.S. 191, 197 (1992); Boos v. Barry, 485 U.S. 312, 318-19 (1988) (plurality opinion) (law regulating speech near a polling place that "depends entirely on whether the speech is related to a political campaign" is content-based); Consolidated Edison Co. v. Public Service Comm'n., 447 U.S. 530, 533, 537 (1980)(law barring the distribution of literature concerning "controversial issues of public policy" is content-based).

[19] Defendants do not oppose plaintiff's request for judicial notice of the fact that certain terrorist attacks have occurred, as listed in the motion. See (Proposed) Order granting judicial notice to facts 2(A)-(I). But defendants do object on evidentiary grounds to reference or reliance on the newspaper articles attached to that motion. See Defendants' Evidentiary Objections filed herewith.

[20] See United States v. Martinez, 904 F.2d 601, 602 (11th Cir. 1990) (designation of cryptographic devices for export control not reviewable since neither the courts nor the parties are privy to reports of the intelligence services on which decision based); United States v. Mandel, 914 F.2d 1215, 1223 (9th Cir. 1990) (determination to regulate export of a particular commodity "are quintessentially matters of policy

which Bernstein cites, underscores the governmental interests at stake.

Moreover, Bernstein acknowledges that he equips millions of Internet users with functioning software. See Bernstein Decl. ¶¶ 63, 70. He thereby concedes that his export activity involves far more than "publishing papers" and merely seeking to convey academic ideas to interested scientists through more precise "language." The government's policy of requiring notice should exporters like Bernstein equip millions of users with powerful encryption does not impermissibly restrict expression, and leaves open broad channels for the publication of cryptographic theory. Ward v. Rock Against Racism, 491 U.S. 781, 802 (1989). See Defs. Mem. at 20-22.[21]/

D. The Overbreadth Doctrine Does not Apply Here.

In the fourteen lines he devotes to the claim, Bernstein fails yet again to demonstrate that the overbreadth doctrine applies in this case. See Pl. Mem. at 21. Defendants have set forth why a facial challenge in general, and an overbreadth claim in particular, are inapplicable here. See Defs. Mem. at 16-17. Bernstein's claim that the EAR encryption provisions have "no conceivable" constitutional application is wrong. See Pl. Mem. at 21. Even assuming, arguendo, the regulations raise concerns as applied to purportedly "academic" interests, they quite properly apply to those who seek to equip millions of computer users with functioning encryption software. Bernstein has failed to establish his standing to vindicate interests other than his own, such as on behalf of enterprises engaged in mass export of commercial encryption. To whatever extent the merits are reached, there is no basis to go

entrusted by the Constitution to the Congress and the President . . ."); United States v. Spawr Optical Research, Inc., 864 F.2d 1467, 1473 (9th Cir. 1988), cert. denied, 493 U.S. 809 (1989) (same). Accord United States v. Moller-Butcher, 560 F. Supp. 550, 553-54 (D. Mass. 1983) (power to restrict export of goods on national security grounds "can (and should) be turned over to the Executive branch, as it has the dominant role in conducting foreign policy"); United States v. Helmy, 712 F. Supp. 1423 (E.D. Cal. 1989) (the designation of export controlled commodities is "the very product of a national security analysis").

[21]/ Plaintiff tries to undercut the government's interest by recycling the regulatory distinction between source code in paper versus electronic form. See Pl. Mem. at 20. That debate has obviously been overtaken by events. The current EAR allows all publicly available electronic encryption source code (and corresponding object code) to be exported after notification or a copy is provided to the government.

beyond any purported application of the regulations to Bernstein's activities.[22]

E. The EAR Encryption Provisions are Not Unconstitutionally Vague.

Plaintiff's First Amendment "vagueness" claim is likewise meritless. See Pl. Mem. at 19-20 and Defs. Mem. at 24-25. His contention that the definitions of encryption and cryptography in the EAR are unclear -- in particular the distinction between "confidentiality" and "authentication" programs – is meritless for the reasons discussed above. See Part I (C) supra. Similarly, the questions that Bernstein raises about the clarity of exclusions for teaching and academic discourse from the EAR are insubstantial, particularly in the absence of any indication that the government seeks to regulate open, public scientific conferences or published discourse on cryptography. See Defs. Mem. at 24-25.

F. The EAR Encryption Provisions are Not a System of Prior Restraint.

Bernstein drops to fourth place in his current motion the "prior restraint" argument that highlighted his prior claims. See Pl. Mem. at 22. This is this is still too high. See Defs. Mem. at 13-16. In particular, Bernstein is wrong that the prior restraint issue may be decided without reference to whether the regulation is content-based. See Pl. Mem. at 23. In Thomas v. Chicago Park District, 122 S. Ct. 775, 779-80 (2002), the Supreme Court made clear that the facial prior restraint doctrine does not apply to laws of general application that do not target the content of speech, such as the revised EAR provisions on encryption software exports. The new requirement of notice or a copy of publicly available encryption being exported presents no prior restraint concerns. See Defs. Mem. at 13-16.

G. The EAR Encryption Provisions Do Not Restrain Free Association.

Next, Bernstein raises his prior assertions that the EAR restricts his association with academics under a "freedom of association" theory. See Pl. Mem. at 24. He equates notice of the export of a software program with an injunction against making a speech on a political subject. Id. The Court can

[22] Bernstein again misconstrues the standing aspect of overbreadth, where a plaintiff must still have a personal injury related to the third party claims he seeks to vindicate. See Secretary of State of Maryland v. Joseph H. Munson Co., 467 U.S. 947, 958 (1984) (plaintiff had standing to challenge requirement on charitable organizations raising funds because it was a fund-raiser). Here, Bernstein's alleged injuries concern application of the regulations to *his* activities. See Los Angeles City Council v. Taxpayers for Vincent, 466 U.S. 789, 802 (1984). Bernstein has no standing to obtain invalidation of the regulations as to other permissible applications, such as to commercial exporters.

decide Bernstein's claims without new constitutional theories. Freedom of association claims typically concern efforts to regulate the activities or membership of an organization, which is not present here.[23]

H. The EAR Encryption Provisions Do Not Violate the Fourth Amendment.

Finally, Bernstein argues that the EAR's requirement of notice for an exported item is an unconstitutional search and seizure under the Fourth Amendment. See Pl. Mem. at 24-25. The authority on which plaintiff relies concerns either warrantless seizures of obscene films or overbroad warrants for political publications. See Roaden v. Kentucky, 413 U.S. 496 (1973) (obscene film seized); Stanford v. Texas, 379 U.S. 476 (1965) (communist literature seized). Here, no issue of seizing software, with or without a criminal warrant, is present. Regulatory requirements on the export of a computer software program do not implicate Fourth Amendment interests, even if First Amendment issues are raised.

CONCLUSION

For the foregoing reasons, defendants' motion to dismiss, or for summary judgment, should granted.

Respectfully Submitted,

ROBERT D. McCALLUM Jr.
Assistant Attorney General

DAVID W. SHAPIRO
United States Attorney

JOCELYN BURTON
California Bar No. 135879
Assistant United States Attorney
450 Golden Gate Avenue
San Francisco, California 94102
Telephone: (415) 436-7198

[23] See Boy Scouts of America v. Dale, 530 U.S. 640 (2000) (inclusion of homosexuals as scout masters); NAACP v. Claiborne Hardware Co., 458 U.S. 886 (1982) (boycott activities of civil rights group); De Jonge v. State of Oregon, 299 U.S. 353 (1937) (communist party membership).

VINCENT M. GARVEY
Deputy Branch Director

____
ANTHONY J. COPPOLINO
Senior Trial Counsel
Department of Justice
Civil Division, Room 1084
901 E Street, N.W.
Washington, D.C. 20530
Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470

Attorneys for the Defendants

CERTIFICATE OF SERVICE

I hereby certify that on August 1, 2002, the foregoing Defendants' Opposition to Plaintiff's Motion for Summary Judgment was served by First Class Mail, postage pre-paid, on:

Sarah E. Pace
McBride Baker & Coles
500 West Madison St. 40th Floor
Chicago, Illinois 60661
(312) 715-5700

Karl Olson
Levy, Ram, Olson & Rossi LLP
639 Front Street, Fourth Floor
San Francisco, California 94111-1913
(415) 433-4949

____
ANTHONY J. COPPOLINO