

1 ROBERT D. McCALLUM Jr.
Assistant Attorney General

2 DAVID W. SHAPIRO
3 United States Attorney

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

7 VINCENT M. GARVEY
8 Deputy Branch Director

9 ANTHONY J. COPPOLINO
Senior Trial Counsel
10 Department of Justice
Civil Division, Room 1084
11 901 E Street, N.W.
Washington, D.C. 20530
12 Tel. (Voice): (202) 514-4782
(FAX): (202) 616-8470

13 Attorneys for the Defendants

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

17 _____)
DANIEL J. BERNSTEIN)

18 Plaintiff,)

19 v.)

20 UNITED STATES DEPARTMENT OF)
21 COMMERCE et al.)

22 Defendants.)
23 _____)

C 95-0582 MHP

**DEFENDANTS' OPPOSITION TO
PLAINTIFF'S MOTION FOR
SUMMARY JUDGMENT.**

Date: October 7, 2002
Time: 2:00 p.m.
Courtroom: 15 [18th Floor]
Chief Judge Marilyn Hall Patel

24
25
26 Submitted: August 2, 2002
27
28

INTRODUCTION

1
2 Plaintiff's motion for summary judgment confirms the jurisdictional and substantive flaws with
3 his Second Supplemental Complaint as set forth in defendants' motion to dismiss, or for summary
4 judgment.^{1/}

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

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

25
26 ^{1/} Hereafter "Pl. Mem." and "Defs. Mem." respectively.

27
28 ^{2/} Indeed, plaintiff only submits one of the advisory opinions. See Tab G to the Declaration of Daniel
J. Bernstein.

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

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

12 PROCEDURAL HISTORY

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

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

27
28 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.

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

4 Plaintiff next asserts that the "Ninth Circuit held that EAR was an unconstitutional prior
5 restraint." Pl. Mem. at 3 (citing Bernstein v. Department of Justice et al., 176 F.3d 1132 (9th Cir.
6 1999)). This is the first of several instances in which plaintiff cites an appellate decision that no longer
7 exists. See Pl. Mem. at 3, 23, 25. As should be obvious, no appellate decision concerning the validity of
8 the prior regulatory regime was ever finalized. When the government's petition for rehearing was
9 granted, the panel decision was withdrawn. Bernstein v. Department of Justice et al., 192 F.3d 1308 (9th
10 Cir. 1999). After superceding regulations were issued, the appeal was remanded without running its
11 course. Defendants obviously had the right to contest the panel decision further had the prior regulations
12 remained in place. Yet plaintiff cites that decision as if it were circuit precedent – even closing his brief
13 with an indented quote from it. Id. at 25.

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

19 CURRENT REGULATORY FRAMEWORK

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

26 1. EAR Encryption Software Provisions

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

1 Fed. Reg. 68572, 68580 (December 30, 1996) (Tab 1 hereto). Along with numerous other items subject
2 to export control, Encryption Items are listed on the Commerce Control List and given classification
3 numbers (called "ECCNs"). See 15 C.F.R. Part 772 (defining ECCN) and Part 774 (ECCN 5A002 for
4 encryption hardware; ECCN 5D002 for encryption software; ECCN 5E002 for encryption technology).
5 Because encryption items "can be used to maintain the secrecy of information and thereby may be used
6 by persons abroad to harm national security, foreign policy, and law enforcement interests," they are
7 subject to export licensing requirements to determine, on a case-by-case basis, whether an export "is
8 consistent with U.S. national security and foreign policy interests." 15 C.F.R. § 742.15(a)(1)(ii). While
9 some exceptions to these license requirements existed in December 1996, they pertained primarily to
10 "mass market" encryption items with limited key lengths, and to "recoverable" encryption products. See
11 61 Fed. Reg. at 68581 (Dec. 30, 1996) (amending 15 C.F.R. § 742.15(b)(1), (2), (3)).

12 **January 2000 Encryption Revisions:** In January 2000, far broader exceptions to encryption
13 license requirements were established for all encryption items, including software and hardware, as set
14 forth in 15 C.F.R. Part 740. See 65 Fed. Reg. 2492-2502 (Jan. 14, 2000) (Tab 2 hereto). In particular, a
15 license exception (called "TSU") was expanded for "unrestricted" encryption source code. Under this
16 exception, encryption source code that would be considered publicly available was excepted from
17 encryption export licensing requirements if they were not commercial items.^{4/} See 15 C.F.R.
18 § 740.13(e), 65 Fed. Reg. at 2497. This license exception was directed at "open source" encryption
19 items – that is, encryption source code made publicly and freely available on the Internet for
20 downloading. See 65 Fed. Reg. at 2492.^{5/}

21 On its face, the expanded license exception for software that would be considered publicly
22 available eliminated requirements that were at the heart of plaintiff's prior claims – specifically, that a
23

24 ^{4/} In the parlance of the EAR, this exception initially applied to software that was "not subject to an
25 express agreement for payment of a licensing fee or royalty for commercial production or sale of any product
26 using the source code." See 15 C.F.R. § 740.13(e), 65 Fed. Reg. at 2497.

27 ^{5/} In October 2000, the EAR encryption provisions were further amended. See 65 Fed. Reg. 62600
28 (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)).

1 license be obtained before Bernstein could freely make his encryption source code available to students,
2 fellow academics, and the world at large on an Internet Web site or newsgroup. Bernstein's claim that,
3 without a license, he could not "publish" his scientific papers containing encryption source code to the
4 Internet no longer exists. The remaining requirement for such exports is that notice be provided by the
5 time of export, either through an email identifying the particular Web site where the software is located,
6 or by providing a copy of the software. See 15 C.F.R. § 740.13(e)(1); 65 Fed Reg. at 2497 (Jan. 14,
7 2000). In addition, although exports of encryption software to certain terrorist designated states
8 remained prohibited, the revised EAR made clear that mere posting to the Internet does not constitute
9 knowledge of such a prohibited export. Id. § 740.13(e)(3), 65 Fed. Reg. at 2497 (Jan. 14, 2000).^{6/}

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

21
22 ⁶ Indeed, under the January 2000 regulations, even *commercial* encryption source code that would be
23 considered publicly available was excepted from general license requirements. See 65 Fed. Reg. at 2498
24 (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
25 65 Fed. Reg. 62600, 62606 (Oct. 19, 2000). Other license exception provisions were expanded in January
26 2000 for exports of certain encryption items to U.S. subsidiaries, for exports to non-government end-users,
27 and for certain "retail" encryption commodities and software. See 65 Fed. Reg. 2497-99 (Jan. 14, 2000)
28 (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).

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

5 2. Encryption Technology Provisions

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

10 By way of background, in addition to regulating the export of specific products (like encryption
11 hardware and software), the EAR also regulates the export of information falling within the definition of
12 technology, *i.e.*, "specific information necessary for the 'development,' 'production,' and 'use' of a
13 product," which may take the form of technical data or technical assistance. See 15 C.F.R. Part 772
14 (definition of technology). Courts have long recognized that export controls may legitimately include
15 the regulation of technology and technical assistance. See United States v. Edler Industries, 579 F.2d
16 516, 522 (9th Cir. 1978); United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989); United States
17 v. Van Hee, 531 F.2d 352 (6th Cir. 1976). The technology provisions of the EAR are solicitous of First
18 Amendment activities by excluding information that is or will be made publicly available, publications,
19 educational information, fundamental research, and academic discussion. See 15 C.F.R. §§ 734.7,
20 734.8, 734.9, 744.9.

21 ARGUMENT

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

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

27 A. Collaboration at Conferences

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

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

7 First, even apart from the exemption from technical assistance in Section 744.9, the EAR
8 otherwise excludes publicly available information from the definition of "technology" – including
9 information exchanged at an open, public conference. See 15 C.F.R. § 734.7(a)(4). Indeed, Bernstein
10 concedes that publicly available "technology" (which is a term defined to include "technical assistance")
11 is not subject to the EAR. See Pl. Mem. at 11. Also, Section 744.9 itself excludes the kinds of
12 exchanges that occur at scientific conferences -- teaching, academic discussion, and the work of groups
13 or bodies engaged in the development of standards -- from the reach of that provision. See 15 C.F.R.
14 § 744.9. From these two provisions, it should be apparent that the EAR does not seek to regulate
15 discourse at open, public scientific conferences, and they have not been so applied to plaintiff.

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

24 Plaintiff cites other provisions of the EAR which he claims impose the same restrictions. The
25 "General Prohibitions" against "re-exports" that plaintiff cites, see Pl. Mem. at 6, on their face apply to
26 "exports subject to the scope of the EAR." See 15 C.F.R. 736.2(b). Transfers of technology to a foreign
27 person outside of the United States through oral communication would not apply to information that is
28 not subject to the EAR to begin with, such as information exchanged at open, public conferences or

1 academic discussions. Also, where the export qualifies for a License Exception under Part 740, it is not
2 restricted by the General Prohibitions. Id.^{7/}

3 Finally, Bernstein also alleges that he cannot collaborate with colleagues at an overseas
4 conference because the general requirement of knowledge for an EAR violation, see 15 C.F.R.
5 § 764.2(e), makes him "vicariously liable" for the "predictable" actions of his foreign colleagues who
6 may take software or technology home with them. See Pl. Mem. at 7-8. This, again, is unfounded. If
7 academic discussion of cryptography at an open, public conference is at issue, the technology and
8 technical assistance provisions of the EAR would not apply to plaintiff or his foreign colleagues, directly
9 or vicariously.

10 B. Notification for Private Email

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

17 C. Notification for "Web Publications"

18 Plaintiff next asserts that, to comply with the notice requirement for exports of encryption to the
19 World Wide Web, he would have to "review all of his desired publications" and "every change to his
20 Web changes" and make as many as three thousand notices per year to comply with the EAR. See Pl.
21 Mem. at 10. This is specious. Bernstein raised this very scenario with the government during the
22 consultation period and was specifically advised that the notice requirement would apply to changes in
23 software where a new encryption algorithm is utilized in the source code whereby an identical input
24

25 ^{7/} For the same reasons, Bernstein's assertion that Section 744.9 and Section 736.2(b)(1) prohibits him
26 from "answering questions" on an Internet newsgroup, see Pl. Mem. at 11, is wrong.

27 ^{8/} Bernstein's September 29, 2001, notification of the Internet location of NISTP224, which contains
28 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.

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

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

19 This distinction is clear in the regulations, as well as technically. The EAR states that
20 "Encryption Items" are those which "can be used to maintain the secrecy of information." See 15 C.F.R.
21 742.15. The applicable Commerce Control List entries for software and hardware that are subject to
22 encryption license controls (ECCN 5D002 and 5A002) expressly exclude items limited to
23 "authentication" -- which is defined to include "all aspects of access control where there is no encryption
24 of files or text except as directly related to the protection of passwords, Personal Identification Numbers
25 (PINs) or similar data to prevent unauthorized access." See ECCN 5A002 (Technical Note 2). It should
26 be obvious, even to a layperson, that software which functions solely to protect PIN numbers or
27 passwords, in order to prevent tampering with a transaction, is different from software that functions to
28 scramble plaintext. It should also be obvious that these different functions have far different national

1 security implications. Bernstein himself sees the distinction between programs that provide "protection
2 against forgery" and those which provide "protection against both forgery and eavesdropping." See
3 Bernstein Decl. ¶¶ 84, 90, 107. For plaintiff to re-plow this ground seven years later is meritless.

4 D. Licensing for Assembly Language Programs

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

14 E. Licensing for Postings to Sci.Crypt

15 Perhaps Bernstein's most egregious assertion is that a license is required to post software to the
16 Internet newsgroup Sci.Crypt because it may be downloaded in Iran or other terrorist nation, and
17 Bernstein "knows" that these postings are available in Iran. The EAR addresses this explicitly and
18 indicates that such postings to the Internet do not constitute knowledge of an impermissible export. See
19 15 C.F.R. § 740.13(e)(6) (as amended by 67 Fed. Reg. at 38862 (June 6, 2002)). The advisory opinions
20 to Bernstein also explicitly address this. See First Advisory Opinion, Tab 3 to Kritzer Declaration at 1.
21 Bernstein's assertion that a license is still required for such postings, without advising the Court of the
22 regulations or advisory opinions, lacks a good faith basis.

23
24 9 In 15 C.F.R. Part 772, the EAR defines: (a) "software" to mean "[a] collection of one or more
25 'programs' or 'microprograms' fixed in any tangible medium of expression; (b) "source code (or source
26 language)" to mean "[a] convenient expression of one or more processes that may be turned by a
27 programming system into equipment executable form ('object code' (or object language)); (c) "encryption
28 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."

1 F. License for Scientific Journals

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

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

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

26 _____
27 ^{10/} He includes in such unspecified costs "author compensation, acquisition costs, editorial costs,
28 illustration costs, design costs, typesetting costs, promotion costs, and profit." Id.

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

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

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

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

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

26 ^{11/} Also, even if priced higher than the cost of production and distribution, the export or reexport of
27 technology or software in a library accessible to the public is not subject to the EAR. See 15 C.F.R. § 734,
28 Supplement No. 1, Question A(5) and § 734.7(a).

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

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

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

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

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

24
25 ^{12/} The Joint Statement of Facts was originally filed, in connection with prior cross-motions, on
26 September 11, 1996 (Docket No. 75) and resubmitted on April 25, 1997 (Docket No. 127).

27 ^{13/} See (Third) Giles Decl. ¶ 9 (4/29/02) (an encryption "source code" is a computer program that
28 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

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

10 Compiling software performs the compiling function and is commonly
11 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.

12 See Joint Statement of Facts ¶ 7 (emphasis added).^{14/}

13 In its first opinion in this case, this Court characterized plaintiff's contention that source code,
14 even as written on paper, should not be considered functional to any extent as "specious" – specifically
15 noting "the ease with which one can convert source code into object code." See Bernstein v. U.S.
16 Department of State, 922 F. Supp. at 1434, n. 14. Other courts have recognized that a computer software
17 program is a set of instructions to a computer that directs computer hardware to perform certain tasks.
18 See Universal City Studios v. Corley, 273 F.3d 429, 449-53 (2d Cir. 2001)("computer code can instantly
19 cause a computer to accomplish tasks"); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1537 n.11 (11th
20 Cir. 1996) and Digidyne Corp. v. Data General Corp., 734 F.2d 1336, 1342 (9th Cir. 1984), cert. denied,
21 473 U.S. 908 (1985) (software is "a set of instructions [to a computer] that allows the system to
22 accomplish a particular task"). See also Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514
23 n.2 (9th Cir. 1993) and Johnson Controls, Inc. v. Phoenix Control Systems, Inc., 886 F.2d 1173, 1175
24 _____
25 electronically in software to transform data into an unintelligible form).

26 ^{14/} In addition, not all source code needs to be "compiled" for execution. For example, "interpreted
27 programs can be executed "on the fly" – underscoring that source code is not merely an "informational"
28 version of software. See (Third) Giles Decl. ¶ 10 (dated 4/29/02).

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

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

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

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

25
26 ^{15/} Circuit Judge Nelson's dissent underscores that the withdrawn panel decision failed to appreciate
27 the functional quality of software in its First Amendment analysis. See Bernstein v. Department of Justice
28 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").

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

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

21
22 ^{16/} Nor can source code accurately be compared to a "chocolate chip cookie recipe." See Pl. Mem. at
23 16. Computer source codes are not instructions which inform people how to mix ingredients; they are
24 instructions to a microprocessor which cause a computer to function a certain way, in this case to encrypt
25 data or text being transmitted through a computer.

26 ^{17/} Examples of scientific articles, textbooks, and open conferences on cryptography, as well as
27 academic courses, have been placed in evidence previously. See Second Declaration of Louis F. Giles III,
28 ¶¶ 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).

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

4 C. The EAR Provisions on Encryption Satisfy Intermediate Scrutiny.

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

17 ^{18/} See City of Cincinnati v. Discovery Network, 507 U.S. 410 (1993) (ordinance barring distribution
18 of "commercial" advertising content-based); Linmark Associates v. Township of Willingboro, 431 U.S. 85
19 (1977) (ordinance forbidding use of specific content -- "For Sale" and "Sold" signs – content based);
20 Burson v. Freeman, 504 U.S. 191, 197 (1992); Boos v. Barry, 485 U.S. 312, 318-19 (1988) (plurality
21 opinion) (law regulating speech near a polling place that "depends entirely on whether the speech is related
22 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).

23 ^{19/} Defendants do not oppose plaintiff's request for judicial notice of the fact that certain terrorist attacks
24 have occurred, as listed in the motion. See (Proposed) Order granting judicial notice to facts 2(A)-(I). But
25 defendants do object on evidentiary grounds to reference or reliance on the newspaper articles attached to
that motion. See Defendants' Evidentiary Objections filed herewith.

26 ^{20/} See United States v. Martinez, 904 F.2d 601, 602 (11th Cir. 1990) (designation of cryptographic
27 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.
28 1990) (determination to regulate export of a particular commodity "are quintessentially matters of policy

1 which Bernstein cites, underscores the governmental interests at stake.

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

9 D. The Overbreadth Doctrine Does not Apply Here.

10 In the fourteen lines he devotes to the claim, Bernstein fails yet again to demonstrate that the
11 overbreadth doctrine applies in this case. See Pl. Mem. at 21. Defendants have set forth why a facial
12 challenge in general, and an overbreadth claim in particular, are inapplicable here. See Defs. Mem. at
13 16-17. Bernstein's claim that the EAR encryption provisions have "no conceivable" constitutional
14 application is wrong. See Pl. Mem. at 21. Even assuming, arguendo, the regulations raise concerns as
15 applied to purportedly "academic" interests, they quite properly apply to those who seek to equip
16 millions of computer users with functioning encryption software. Bernstein has failed to establish his
17 standing to vindicate interests other than his own, such as on behalf of enterprises engaged in mass
18 export of commercial encryption. To whatever extent the merits are reached, there is no basis to go
19
20

21
22 entrusted by the Constitution to the Congress and the President . . ."); United States v. Spawr Optical
23 Research, Inc., 864 F.2d 1467, 1473 (9th Cir. 1988), cert. denied, 493 U.S. 809 (1989) (same). Accord
24 United States v. Moller-Butcher, 560 F. Supp. 550, 553-54 (D. Mass. 1983) (power to restrict export of
25 goods on national security grounds "can (and should) be turned over to the Executive branch, as it has the
26 dominant role in conducting foreign policy"); United States v. Helmy, 712 F. Supp. 1423 (E.D. Cal. 1989)
27 (the designation of export controlled commodities is "the very product of a national security analysis").

28 ^{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.

1 beyond any purported application of the regulations to Bernstein's activities.^{22/}

2 E. The EAR Encryption Provisions are Not Unconstitutionally Vague.

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

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

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

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

20 Next, Bernstein raises his prior assertions that the EAR restricts his association with academics
21 under a "freedom of association" theory. See Pl. Mem. at 24. He equates notice of the export of a
22 software program with an injunction against making a speech on a political subject. Id. The Court can
23

24 ^{22/} Bernstein again misconstrues the standing aspect of overbreadth, where a plaintiff must still have
25 a personal injury related to the third party claims he seeks to vindicate. See Secretary of State of Maryland
26 v. Joseph H. Munson Co., 467 U.S. 947, 958 (1984) (plaintiff had standing to challenge requirement on
27 charitable organizations raising funds because it was a fund-raiser). Here, Bernstein's alleged injuries
28 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.

1 decide Bernstein's claims without new constitutional theories. Freedom of association claims typically
2 concern efforts to regulate the activities or membership of an organization, which is not present here.^{23/}

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

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

11 CONCLUSION

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

14 Respectfully Submitted,

15 ROBERT D. McCALLUM Jr.
Assistant Attorney General

16 DAVID W. SHAPIRO
United States Attorney

17
18 JOCELYN BURTON
California Bar No. 135879
19 Assistant United States Attorney
450 Golden Gate Avenue
20 San Francisco, California 94102
Telephone: (415) 436-7198

21
22
23
24
25
26 ^{23/} See Boy Scouts of America v. Dale, 530 U.S. 640 (2000) (inclusion of homosexuals as scout
27 masters); NAACP v. Claiborne Hardware Co., 458 U.S. 886 (1982) (boycott activities of civil rights group);
28 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

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

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

7/0], this Court should deny Plaintiffs Motion for Summary Judgment, decline to issue declaratory judgment or injunctive relief, and dismiss the Complaint. Respectfully submitted, BRIAN FROSH.Â CERTIFICATE OF SERVICE I certify that on August 2, 2019, I served a copy of this Opposition and its exhibit by first class mail, postage prepaid, to: Daniel B. Rice, Esq. Nicholas Y. Riley, Esq. Institute for Constitutional Advocacy and Protection Georgetown University Law Center 600 New Jersey Ave. Defendantsâ€™ Opposition To Plaintiffsâ€™ Motion for Summary Judgment maintains that this Court lacks jurisdiction to decide whether the Defendantsâ€™ regulations are ultra vires; that the Plaintiffsâ€™ claims are not ripe for judicial review; that the Plaintiffs are unlawfully joined; and that this court lacks authority to review Defendantsâ€™ regulations because they are entitled to Chevron-type.Â The Plaintiffs respectfully disagree with each of these contentions. This court has jurisdiction over plaintiffsâ€™ claims. Defendantsâ€™ claim that Plaintiffs have not identified â€œany waiver of sovereign immunityâ€ which allows this court to assume jurisdiction over this case. See Defendantsâ€™ Opposition, pp. 12-13. Five Approaches To Opposing A Motion For Summary Judgment: Show that the motion fails to list the specific facts and law supporting summary judgment. A lazy or sleazy lawyer will submit a motion consisting of boilerplate language from Rule 56, or the state equivalent, with little or no reference to the facts of the case. You can challenge that lack of specifics using your stateâ€™s rules of civil procedure on summary judgments.Â Well the new reappointed Judge ended up denying the Plaintiffâ€™s motion for Rehearing/Reconsideration of the Order on my Motion to Compel. He upheld the prior Judgeâ€™s order granting my Motion to Compel, and gave the Plaintiff until the 21st to produce the documents I listed in my discovery request. 124 000 Plaintiff's Opposition to Defendant AU MD Sports Med Motion for Summary Judgment and Cross Motion for Summary Judgment. Item Preview. There Is No Preview Available For This Item. This item does not appear to have any files that can be experienced on Archive.org. Please download files in this item to interact with them on your computer. Show all files. remove-circle. Share or Embed This Item. EMBED.Â Identifier. 6567296-124-000-Plaintiff-s-Opposition-to-Defendant-AU. Scanner. Internet Archive Python library 1.8.5. Source. <http://www.documentcloud.org/documents/6567296-124-000-Plaintiff-s-Opposition-to-Defendant-AU.html>. plus-circle Add Review. comment.