

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)

19 Plaintiff,)

20 v.)

21 UNITED STATES DEPARTMENT OF)
COMMERCE et al.)

22 Defendants.)
23)

C 95-0582 MHP

**DEFENDANTS' REPLY TO
PLAINTIFF'S OPPOSITION TO
DEFENDANTS' MOTION TO
DISMISS OR, IN THE ALTERNATIVE,
FOR SUMMARY JUDGMENT**

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

24
25
26
27 Submitted: September 2, 2002

INTRODUCTION

1
2 The Court is well familiar with the issues in this long-standing case and, as such, in this final
3 reply, defendants will summarize the core points in dispute and rebut the main contentions in plaintiff's
4 opposition brief ("Pl. Opp. ").

5 The key issue in this case is whether the United States Government may, consistent with the
6 Constitution, regulate in some manner the export of encryption software in source code form. The
7 extent of that regulation has changed significantly since this case started, but plaintiff's theories have
8 changed very little. Plaintiff contends that, because encryption software programs, at least in source
9 code form, convey scientific ideas as to how the program operates, restrictions on their export violate the
10 First Amendment. In addition, plaintiff also claims that related provisions in the Export Administration
11 Regulations ("EAR") concerning the export of "technical assistance" and "technology" also
12 unconstitutionally restrict his ability to convey scientific ideas about cryptography.

13 While plaintiff's numerous regulatory interpretations and constitutional theories leave much to
14 untangle, the central factor in this case – and the one that drives the constitutional analysis – is that
15 encryption software programs, while informative to some, also *perform* a technical function to encrypt
16 data on a computer. In this round of motions, plaintiff recognizes that this is a core issue in this case.
17 But the argument he stresses – that encryption software programs are mere "utility" speech, like
18 technical manuals, blueprints, cooking recipes, or even music – is wrong. There is no genuine issue of
19 fact that a source code program is not simply expressive of "ideas" that have "utility," but an item that
20 provides an actual technical capability to encrypt data on a computer.

21 The government's interest in the export of encryption software and hardware exists because the
22 technical capability to conceal information through encryption can have a significant and debilitating
23 impact on national security. See (Third) Declaration of Louis F. Giles (filed April 29, 2002) ¶ 7. As
24 such, a core activity carried out by the National Security Agency is "cryptanalysis" – the science of
25 reading "cipher text" (*i.e.*, determining the content of encrypted messages). Id. ¶ 7. History has
26 demonstrated the critical importance of the government's ability to decipher communications.
27 Cryptography historian David Kahn has written that "[i]n World War II, cryptanalysis helped make
28 possible at least four critical events," including the U.S. victory at the Battle of Midway and the defeat of

1 U-boat attacks against the United States and its allies.^{1/} The government deals with national security
2 threats in many ways, and one tool is to regulate the export of encryption hardware and software that
3 might fall into the hands of foreign adversaries. Notice of such exports, in particular, assists in efforts to
4 deal with encryption encountered overseas. See Giles Decl. ¶¶ 15-17.

5 There is nothing unconstitutional about tracking the export of encryption. The ideas inherent in
6 encryption software – cryptographic algorithms themselves and theoretical discussions about the
7 mathematical functions underlying cryptography – are broadly disseminated. The opening line of
8 plaintiff's opposition brief – that the EAR was amended in 1996 "to control the science of cryptography,"
9 see Pl. Opp. at 1 – is absurd. It was not true in 1996, and it is not true now. The science of cryptography
10 is flourishing – with conferences, courses, textbooks, journal articles, and published algorithms
11 abounding. The Export Administration Regulations are solicitous of this activity. Regulating the export
12 of items that *perform* encryption does not unconstitutionally restrict the expression of ideas *about*
13 encryption. Moreover, regulating the export of technology and technical assistance related to building
14 products overseas has long been recognized as lawful, and these provisions of the EAR specifically
15 exclude from their reach scientific and academic discourse and publication.

16 These are the overarching considerations that should govern the outcome of this case. But there
17 are also several, more specific, concerns raised by plaintiff's Second Supplemental Complaint. Plaintiff
18 entirely discounts the change in encryption export controls since 1995, in which the government's policy
19 has moved from treating all encryption items for export as if they were munitions, to one which simply
20 requires an email notice when encryption source code and its corresponding object code is posted to the
21 Internet. Plaintiff also persists in disregarding the formal advisory opinions the government provided
22 him during the Court-sponsored period in 2001 for attempting to resolve this dispute. These opinions
23 were not mere "words," see Pl. Opp. at 7, but formal advice from the government's regulatory authority
24 indicating that the EAR does not seek to restrict academic activities. In addition, plaintiff has not
25 identified software at issue in his current challenge that is even subject to the EAR encryption
26 provisions. For these reasons, the Second Supplemental Complaint presents threshold jurisdictional

27
28 ^{1/} See, Chapter 15 of The Codebreakers, by David Kahn, published by The Macmillan Company,
Copyright 1973, at page 339, attached to Third Declaration of Anthony Coppolino.

1 issues. Even if the merits are reached, the EAR encryption provisions are a content-neutral law of
2 general application that serves significant governmental interests in regulating the export of U.S.-origin
3 items that have national security significance, and they do so without impermissibly restricting speech.

4 ARGUMENT

5 **I. PLAINTIFF FAILS TO DEMONSTRATE A JUSTICIABLE CASE OR** 6 **CONTROVERSY.**

7 During this round of motions, defendants have raised both jurisdictional and merit defenses, as
8 they have previously.^{2/} As to jurisdiction, defendants' position is based on two circumstances:
9 (i) plaintiff's failure to identify encryption software at issue; and (ii) plaintiff's disregard of the guidance
10 provided to him by the government.

11 First, defendants noted that plaintiff's Second Supplemental Complaint raised standing and
12 ripeness concerns because plaintiff never sought to demonstrate that the software he now puts at issue is
13 subject to the regulations challenged. See Def. Mem. at 7-8.^{3/} Later, defendants pointed out that, so far
14 as could be determined from public sources, plaintiff's software is not subject to the EAR. See Def.
15 Opp. at 1, 12^{4/} and Second Declaration of Bernard Kritzer. As such, plaintiff's challenge to the
16 encryption software provisions of the EAR does not present the kind of concrete controversy on which
17 Article III jurisdiction may be based. See Def. Mem. at 7-8. Absent a showing that encryption software
18 subject to the EAR is at issue, the Court would be rendering an advisory opinion as to the regulations as
19 they might generally apply to encryption software exports. Such an opinion would be unmoored from
20 the context of a specific dispute over an export activity or software program. Plaintiff had two years to
21 perfect his current challenge and failed to do so, despite clear warning. If plaintiff later develops
22 encryption software that is subject to the EAR, and he wishes to challenge any requirements related to its

23
24 ^{2/} Plaintiff finds some meaning in the "similarity" of positions defendants have taken previously and
25 in this round. See Pl. Opp. at 1-2. That should come as no surprise. Because of intervening regulatory
26 changes, plaintiff's claims in this case have never been finally adjudicated, and his Second Supplemental
27 Complaint raises theories quite similar to those raised earlier.

28 ^{3/} "Def. Mem." refers to Defendants' Memorandum of Points and Authorities in Support of Defendants'
Motion to Dismiss or, in the Alternative, for Summary Judgment.

^{4/} "Def. Opp." refers to Defendants' Opposition to Plaintiff's Motion for Summary Judgment.

1 export, he could seek to file suit at that time.^{5/}

2 Defendants have also made a second, and broader, jurisdictional point. Plaintiff makes numerous
3 specific claims regarding the EAR provisions on both encryption software and technology that are
4 contrary either to the regulations, or the government's advisory opinions, or both. See Def. Mem. at 9-
5 10. Despite an express license exception implemented in January 2000, plaintiff continues to claim that
6 the EAR requires a license to post encryption source code to the Internet, including to a newsgroup
7 where it might be accessible in Iran. Plaintiff's claim that he must obtain a license to "mirror" software
8 already publicly available on the Internet is also baseless. Plaintiff's claim that the EAR restricts his
9 "collaboration" at conferences, or require the production of private email, or prohibit the publication of a
10 book, are likewise contrary to the regulations or express guidance he received from the government.

11 This should not simply be passed over as "merits" issues. The types of allegations made by
12 plaintiff warrant a jurisdictional challenge. Where something is no longer required by revised
13 regulations (e.g. license no longer required to post encryption source code publicly to the Internet), or the
14 government, in response to a formal request, indicates that something is not regulated (license not
15 required for "mirroring" software already publicly available on the Internet or for posting to the publicly
16 available sci.crypt newsgroup), claims that license requirements *still exist* are based on unfounded
17 conjecture and speculation, and not on a credible threat of prosecution. Laird v. Tatum, 408 U.S. 1, 13-
18 14 (1972); City of Los Angeles v. Lyons, 461 U.S. 95, 102 (1983); O'Shea v. Littleton, 414 U.S. 488,
19 494 (1974); Thomas v. Anchorage Equal Rights Commission, 220 F.3d 1134, 1139 (9th Cir. 2000). See
20 Def. Mem. at 9-10.^{6/}

21 Plaintiff attempts to deal with this authority by first alleging he has "a concrete plan to violate the
22 EAR" and that he has been "threatened with prosecution." Pl. Opp. at 5-6. The first contention is
23 meritless, the second specious, and both are little more than post-hoc rationalizations designed to address
24

25 ^{5/} Even plaintiff's original "snuffle" software is no longer subject to license requirements since it is
26 publicly available and the government long ago received a copy.

27 ^{6/} While plaintiff discounts the advisory opinions as mere "words," Pl. Opp. at 7, not every detail of
28 export activities can be accounted for in general regulatory provisions. Accordingly, the EAR provides a
formal process to answer questions on proposed export activities. See 15 C.F.R. § 748.3.

1 the case law on standing. Turning that law on its head, plaintiff's "concrete plan to violate" the EAR is
2 *based on* his own conjecture as to what the EAR requires. As defendants have addressed in detail,
3 plaintiff's claims as to what the EAR requires run contrary to both the regulations and the specific
4 guidance he has received. See Def. Opp. at 6-12. To obtain standing under the "concrete plan to violate
5 the law" theory, the alleged violations must not be conjectural.^{7/}

6 Plaintiff's second assertion – that he has been threatened with prosecution – is likewise without
7 foundation. A threat of enforcement must at least be "credible," not simply "imaginative or speculative."
8 Anchorage Equal Rights, 220 F.3d at 1140 (quoting Babbitt v. United Farm Workers, 442 U.S. 289, 298
9 (1979)). The fact that the Commerce Department continues to "review and license encryption items
10 under the EAR, and enforce violations of the regulations," see Pl. Opp. at 4 and Exhibits A and B to the
11 Bernstein Declaration in Opposition, says nothing about whether *plaintiff's* proposed activities would
12 require a license or violate the EAR. See Def. Opp. at 6-12. The mere existence of a regulatory scheme,
13 and alleged "chill" based on speculation as to its application, does not support standing.^{8/}

14 Plaintiff's effort to fabricate a threat of prosecution is specious. He first cites opinions he
15 received from the government which describe when the notice requirement for encryption software
16 exports would apply. See Pl. Opp. at 5-6 (citing Advisory Opinion at Attachment 5 to First Kritzer
17 Declaration). Advice that plaintiff *voluntarily* solicited, and which indicates what regulations generally
18 provide, hardly constitutes a "threat of prosecution," or an indication that prosecution of the plaintiff is

19 ^{7/} Moreover, even if it was clear that certain activities were prohibited by law, the Ninth Circuit has
20 held that a professed "general intent to violate a statute at some unknown future date does not rise to the
21 level of an articulated, concrete plan." Anchorage Equal Rights, 220 F.3d at 1139; San Diego County Gun
22 Rights Comm. v. Reno, 98 F. 3d 1121, 1126-27 (9th Cir. 1996) (intent to engage in proscribed conduct fails
to demonstrate that alleged threat of prosecution was reasonable).

23 ^{8/} In Steffel v. Thompson, 415 U.S. 452 (1974), the Supreme Court found alleged threats of
24 prosecution to be credible where the plaintiff had twice been stopped by police for distributing handbills and
25 was expressly warned that if he disobeyed he would likely be prosecuted. Id. at 459. In City of Los Angeles
26 v. Lyons, supra, the Supreme Court refused to find standing to challenge future application of a "choke-hold"
27 policy by police where the plaintiff had previously been choked by police under the policy. 461 U.S. at 102-
28 105. In O'Shea v. Littleton, supra, the Supreme Court declined to find standing to challenge future
discriminatory criminal law enforcement where the plaintiffs claimed they had actually suffered
unconstitutional practices, finding that past wrongs were not evidence of "where there is real and immediate
threat of repeated injury." 414 U.S. at 495-96. Here, plaintiff's basis for standing is far weaker, since he has
never been prosecuted or threatened with prosecution based on his purported export activities.

1 likely under the regulations. This is especially so where the full weight of that advice indicates that
2 plaintiff's proposed activities do not require an export license.

3 Plaintiff's allegation that an email from defendants' counsel to plaintiff's counsel was a threat of
4 prosecution is a particularly gross mischaracterization. See Exhibit D to Declaration of Daniel J.
5 Bernstein in Opposition to Defendants' Motion for Summary Judgment. That communication was in
6 response to a request that the government stipulate to the entry of a preliminary injunction and, in the
7 process, agree to a blanket exemption as to any export activity plaintiff might undertake at a conference,
8 including exporting or re-exporting encryption software, wholly without regard to the requirements of
9 the EAR. See Exhibit D to Bernstein Declaration in Opposition. Quite obviously, defendants could not
10 agree to exempt plaintiff from the law, including as to encryption software exports, when it had no idea
11 what the full scope of his intended activities would be. Id. But defendants' communication added:

12 [A]s Dr. Bernstein has been informed by advisory opinions,
13 and the EAR make clear, academic activities, including
14 discussions of encryption technology, at conferences in the
15 United States and abroad, are freely permitted by the EAR.

16 Id. The email by defendants' counsel went on to state that, with respect to the export of encryption
17 software, the principle requirement at issue is to notify the government of certain exports, but that, since
18 the conferences would apparently occur in the United States and Canada, even this requirement may not
19 apply. Id. To suggest that this communication constitutes a "threat of prosecution" is entirely
20 unfounded.^{2/}

21 The bottom line on the jurisdictional issues in this case is that: (1) plaintiff has failed to show
22 that his software is subject to the EAR, and (2) even if it were, his claims that a license is still required to
23 post encryption software to the Internet, collaborate with colleagues, or publish a book, are based on his
24 own conjecture. The Court can and should dismiss plaintiff's Second Supplemental Complaint on
25 jurisdictional grounds.

26 ^{2/} Having cited defendants' March 4, 2002, email as a "threat" to prosecute him, Bernstein wonders why
27 the government has not responded to his May 16, 2002, letter which again requested a stipulation. By this
28 time, the Court itself had indicated at the March 5, 2002, status conference that it saw no basis for
preliminary injunctive relief, and the government had already advised plaintiff of its views four times,
including specifically its position on a stipulation.

1 **II. THE EAR PROVISIONS ON THE EXPORT OF ENCRYPTION SOFTWARE ARE A**
2 **CONTENT-NEUTRAL LAW OF GENERAL APPLICABILITY THAT SERVE A**
3 **SUBSTANTIAL GOVERNMENTAL INTEREST AND DO NOT IMPERMISSIBLY**
4 **RESTRICT EXPRESSION.**

5 Plaintiff makes separate but related arguments that the notification requirement for some
6 encryption software exports burdens spontaneous speech, and is a content-based restriction that does not
7 serve a compelling governmental interest. See Pl. Opp. at 9-17. This disjointed discussion, while
8 meritless, at least joins the battle on the proper ground.

9 **1. The EAR Software Provisions Are Not Directed At the Content of**
10 **"Utility" Speech Comparable to Cooking Recipes.**

11 The initial, overriding issue in assessing plaintiff's First Amendment claim is whether the notice
12 provision for encryption software exports is directed at the content of speech. Plaintiff hinges his case
13 on the theory that a software program in source code form is merely speech that has "utility" which fairly
14 may be compared to "For Sale" signs, sheet music, player-piano rolls, street maps, blueprints,
15 cookbooks, car-repair manuals, murder-for-hire instructions, and even a mushroom encyclopedia. See
16 Pl. Opp. at 11-14. This is the heart of plaintiff's First Amendment analysis, and it is wrong.

17 As defendants have set forth, see Def. Opp. at 13-14, there is no genuine issue of fact that a
18 software program is not simply expressive of ideas that have utility, but an item that implements those
19 ideas to provide an actual technical capability. Courts have routinely recognized the functional quality
20 of software. See id. Even if expressive of ideas for those able to understand programming language, the
21 actual technical function that software provides separates it from speech such as music or a cookbook.
22 What plaintiff labels the content of "documents" containing "instructions" that provide "utility" is
23 actually a software program that contains instructions to a computer microprocessor that causes the
24 computer hardware to function a certain way – in the case of encryption, to transform plaintext into
25 ciphertext. No matter how plaintiff spins the issue, he cannot escape the fact that encryption software
26 programs function to encrypt data on a computer. This sets them apart fundamentally from casserole
27 recipes, books about mushrooms, music, player pianos, or the front page of The New York Times.

28 Even to the degree that encryption source code programming language may be considered
scientific expression under the First Amendment, where a regulation does not target the content of ideas,
and only incidentally restricts such speech in furtherance of a substantial governmental interest, while

1 leaving open ample channels to convey ideas, it passes First Amendment scrutiny. That is the case here.

2 The regulations at issue are, on their face, not directed at the content of ideas, but at the export of
3 both encryption hardware and software items – among dozens of other items controlled for national
4 security or foreign policy reasons on the Commerce Control List. See 15 C.F.R. Part 774; Def. Mem. at
5 15, 18; Def. Opp. at 16. The regulations make no reference to limiting the spread of ideas about the
6 science of cryptography and, indeed, specifically exempt the publication of information from regulation.
7 See Def. Mem. at 19; Def. Opp. at 16 and n.17.^{10/}

8 Moreover, the notice provision applicable to the export of publicly available encryption source
9 code and its corresponding object code does not restrict exports based on the content of ideas – since it is
10 not a restriction at all. The government does not purport to judge what software may or may not be
11 posted publicly to the Internet, based on its content or otherwise. All encryption source code (and its
12 corresponding object code) that would be considered publicly available can be exported under a license
13 exception. See 15 C.F.R. § 740.13(e) (License Exception TSU). The government requires only a copy
14 of the software or an email identifying where the software can be found on the Internet. Id.
15 § 740.13(e)(5). The government does not, through this provision, exercise any discretion that limits
16 exports based on the content of the software.

17 As such, the notice provision in no way compares to the restrictions found impermissible in cases
18 on which plaintiff relies. Those cases concern an advance registration requirement before individuals
19 could engage in pure speech activities, such as parades, demonstrating in a park, leafleting in airports, or
20 distributing religious literature in neighborhoods.^{11/} The notice requirement on the export of encryption
21 software does not require that people register or obtain a permit to speak; it requires that they send the

23 ^{10/} Indeed, the government itself published the content of a significant cryptographic algorithm -- the
24 Data Encryption Standard. See Federal Information Processing Standards Publication 46 (January 15, 1977)
(Tab 10 to Crowell Declaration) (dated 7/26/96) (Docket No. 95).

25 ^{11/} See Rosen v. Port of Portland, 641 F.2d 1241 (9th Cir. 1981) (rejecting one day advance notice
26 requirement and registration before leafleting at airport); Grossman v. City of Portland, 33 F. 3d 1200 (9th
27 Cir. 1994) (rejecting application requirement before protesting in public park); NAACP Western Region v.
28 City of Richmond, 743 F.2d 1346 (9th Cir. 1984) (rejecting requirement for parade permit application 20
days in advance of parade); Watchtower Bible and Tract Society of New York v. Village of Stratton, 122
S. Ct. 2080 (2002) (rejecting ordinance requiring an advance permit before door-to-door advocacy).

1 government a copy of encryption software that they are transmitting to the world, or a notification of its
2 Internet location. The export of functional software is a far different scenario from adherents of
3 Jehovah's Witness going door-to-door, or people protesting in a park, marching against race
4 discrimination, or leafleting at an airport. Indeed, plaintiff now concedes that his exports of software are
5 not mere conveyances of academic ideas to fellow scientists in precise programming language, but that
6 millions world-wide use his software on their computers. See Declaration of Daniel J. Bernstein in
7 Support of Plaintiff's Motion for Summary Judgment ¶¶ 63, 70.

8 **2. The Governmental Interest at Stake is Substantial.**

9 Next, plaintiff derides the governmental interests at stake as "spying," and dismisses as
10 "speculative" the idea that lives can be saved by a policy that assists the government in preparing to deal
11 with encryption capabilities it may encounter. See Pl. Opp. at 16. In particular, he cites successful
12 terrorists attacks as evidence that the government has no valid interest at stake. Id. Bernstein's
13 assertions are meritless. He cannot genuinely dispute that powerful encryption conceals data. See Giles
14 Decl. ¶ 5. He cannot genuinely dispute that the government works to find out what hostile foes are
15 doing and advise senior national security leaders. Id. ¶ 4. He cannot genuinely dispute that, in the
16 wrong hands, the use of encryption by foreign intelligence targets can have a debilitating effect on
17 NSA's ability to collect and report critical foreign intelligence. Id. ¶ 6. And he cannot genuinely dispute
18 that a core NSA activity is cryptanalysis. Id. ¶ 7. Notice of which powerful U.S.-origin encryption items
19 are leaving this country is an important tool in that effort. Id. ¶¶ 15-17.

20 We know that people and organizations who would do harm to the United
21 States are using encryption products and services. Thus, it is imperative
22 that the Government has as much understanding as possible of encryption
23 products that may be used by foreign adversaries. In order to assist in
24 overcoming encryption for foreign intelligence purposes it is necessary to
25 determine what encryption has been employed and how the encryption
26 product is applied to the user's data.

27 Giles Decl. ¶ 16. This is a plainly well-founded, rational basis for the notice requirement as to
28 encryption exports.

For reasons which should be obvious, the government cannot detail its signal intelligence
activities and successes, which are among the most classified national security information. See Halkin
v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978). However, the historical record that is available should assist

1 the Court in recognizing the critical value of signals intelligence and cryptanalysis in national security
2 matters. For example, in an insightful chapter on the role of signals intelligence and cryptanalysis
3 during World War II, historian David Kahn describes the invaluable assistance that code-breaking
4 provided in the crucial U.S. victory at the Battle of Midway.^{12/} Through persistent cryptanalysis, the
5 U.S. Navy learned specific details of the planned Japanese attack on Midway Island, and were able to
6 surprise and destroy the core of the Japanese fleet.

7 "Midway was essentially a victory of intelligence," [Admiral] Nimitz has
8 written. "In attempting to surprise, the Japanese themselves were
9 surprised." General Marshall was even more specific: As a result of
10 cryptanalysis, he declared, "We were able to concentrate our limited forces
11 to meet their naval advance on Midway when otherwise we almost
12 certainly would have been some 3,000 miles out of place."

13 David Kahn, *The Codebreakers*, at 314. Kahn adds: "The codebreakers . . . had engrossed the fate of a
14 nation. They had determined the destinies of ships and men. They had turned the tide of the war. They
15 had caused a Rising Sun to start to set." *Id.* Kahn concludes that, in World War II, "[c]ryptanalysis was
16 not just a tangential and merely helpful factor; it was a vital one." *Id.* at 340.^{13/}

17 The fact that those who would do harm to America sometimes succeed is not, as plaintiff argues,
18 see Pl. Opp. at 16, grounds to find that the government has no substantial interest in utilizing tools that it
19 believes will assist in protecting national security. While, again, the government's successes in this area
20 cannot be disclosed, success in every instance is not the measure of the adequacy of the governmental
21 interest at stake; rather, it is the *need* to protect against the very dangers plaintiff cites that underscores
22 the significance of the government's interest. Moreover, courts have recognized and respected such
23 national security concerns, particularly as related to export controls. See Def. Opp. at 17 n.20. As one
24 court noted specifically with respect to the export of encryption devices:

25 Neither the courts nor the parties are privy to reports of the intelligence
26 services on which this decision, or decisions like it, may have been based.
27 Chicago & Southern Air Lines [v. Waterman SS. Corp.], 333 U.S. [103,]
28 111 [(1948)]. The consequences of uninformed judicial action could be
grave. Questions concerning what perils our nation might face at some

26 ^{12/} See Chapter 15 of *The Codebreakers*, by David Kahn, published by The Macmillan Company,
27 Copyright 1973, at pages 299-314 attached to the Third Coppolino Declaration.

28 ^{13/} If the Court is to take "judicial notice" of successful terrorist attacks as plaintiff requests, it should
also take notice of the significance of cryptanalysis that can be gleaned from the historical record.

1 future time and how best to guard against those perils "are delicate,
2 complex, and involve large elements of prophecy. They are and should be
3 undertaken only by those directly responsible to the people whose welfare
4 they advance or imperil. . . ." *Id.*

5 United States v. Martinez, 904 F.2d 601, 602 (11th Cir. 1990).^{14/} So long as ample alternative channels
6 of expression are available to convey ideas about cryptography, Ward v. Rock Against Racism, 491 U.S.
7 781, 802 (1989), requiring notice as to *when* encryption software is exported publicly on the Internet
8 does not inhibit free expression -- indeed, it does not restrict its world-wide dissemination at all.

9 **III. THERE IS NO BASIS FOR FACIAL INVALIDATION OF THE EAR ENCRYPTION**
10 **PROVISIONS ON PRIOR RESTRAINT OR OVERBREADTH GROUNDS.**

11 Plaintiff continues to overreach by seeking *facial* invalidation of the EAR's encryption provisions
12 in *all* their applications. These claims cannot be justified based on Bernstein's own interests, and are not
13 supported by the law. See Def. Mem. at 12, 13-16.

14 **1. Facial Prior Restraint:** Plaintiff's contention that his facial prior restraint claim in this case
15 survives the Supreme Court's recent decision in Thomas v. Chicago Park District, 122 S. Ct. 775 (2002),
16 is meritless. There, the Court explained that the holding of Freedman v. Maryland, 380 U.S. 51 (1965),
17 on which plaintiff has so heavily relied, does not apply where the law in question "does not authorize a
18 licensor to pass judgment on the *content* of speech," *id.* at 779 (emphasis added), and where "the object
19 of the permit system . . . is not to exclude communication of a particular *content*." *Id.* at 779-80
20 (emphasis added). Chicago Park District is consistent with the Supreme Court's prior decision in City of
21 Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750 (1988), which itself squarely held that "a facial
22 challenge lies whenever a licensing law gives a government official or agency substantial power to
23 discriminate based on the *content or viewpoint* of speech by suppressing disfavored speech or disliked
24 speakers." 486 U.S. at 759. Thus, even under Lakewood, if a law is not directed at the content of ideas
25 or disfavored speakers, a facial prior restraint analysis does not lie.

26 Moreover, the Court in Chicago Park District distinguished another facial prior restraint case on

27 ^{14/} Accordingly, plaintiff's evidentiary objections to the Declaration of Louis Giles of the National
28 Security Agency is baseless. See Plaintiff's Evidentiary Objections to Giles Declaration and Motion to
Strike. For purposes of articulating the governmental interest at stake, officials of the National Security
Agency are clearly qualified to identify the central significance of signals intelligence and cryptanalysis in
national security matters, and the importance of the notice requirement for encryption exports.

1 which plaintiff relies, FW/PBS v. City of Dallas, 493 U.S. 215 (1990), by noting that FW/PBS like
2 Freedman, involved ordinances which targeted business engaged in sexually explicit speech. See
3 Chicago Park District, 122 S. Ct. at 780 n.2. Such laws were subject to facial challenge precisely
4 because they were directed at, or motivated by, the goal of censoring a particular content of speech. The
5 Lakewood-Freedman-FW/PBS line of authority does not apply to content-neutral regulations. See
6 Bernstein v. Department of Justice et al., 176 F.3d 1132, 1147-50 (9th Cir. 1999) (Nelson, J. dissenting).

7 Plaintiff's contention that the Court in Chicago Park District decided that case on facial prior
8 restraint grounds, see Pl. Opp. at 20, is not accurate. In deciding the merits, the Court first relied on an
9 *intermediate-review case*, Clark v. Community for Creative Non-Violence, 468 U.S. 288 (1984), noting
10 that there was no dispute that the ordinance at issue in Chicago Park District was content-neutral,
11 narrowly tailored, and left open ample channels of communication. Chicago Park District, 122 S. Ct. at
12 780 n.3. That is the standard of review applicable here. The Court went on to examine solely the issue
13 of whether the government's discretion was unlimited in deciding whether to grant a permit for large-
14 scale events in public parks, and found that the permit system did not vest so much discretion to warrant
15 invalidation. Id. at 780-81. In this case, all encryption source code (and its corresponding object code)
16 that would be considered publicly available is eligible for a licence exception. Under Chicago Park
17 District, the EAR notice requirement for the export of encryption software leaves no discretion in a
18 licensing official to censor the content of certain information.

19 **2. Overbreadth:** Plaintiff's opposition brief demonstrates that he still does not state a valid
20 overbreadth claim. Bernstein alleges that the "EAR, as applied to Prof. Bernstein's desired activities, is
21 an unconstitutional content-based regulation. . . . For the same reasons, EAR, on its face, is an
22 unconstitutional content-based regulation of speech." See Pl. Opp. at 17 (emphasis added). Bernstein's
23 claim is quite clear: he alleges that, because the EAR applies to *his* desired activities, it is also
24 "overbroad." This is obviously an as-applied claim. The Supreme Court has rejected plaintiff's
25 conception of an overbreadth claim at least twice. Los Angeles City Council v. Taxpayers for Vincent,
26 466 U.S. 789, 802-03 (1984); Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 502 (1984) (overbreadth
27 doctrine does not apply where plaintiff himself "desire[s] to engage in protected speech that the
28 overbroad statute purports to punish," since, in such a circumstance, there is "no want of a proper

1 party").^{15/}

2 Plaintiff's assertion that EAR provisions on encryption have no legitimate sweep, see Pl. Opp. at
3 17, is frivolous. Export controls apply largely to commercial exporters, and plaintiff has no standing to
4 vindicate their interests, or any basis on which to allege that, as to such enterprises, the regulation of
5 encryption exports is an impermissible restriction on "speech." The very exhibit plaintiff submits with
6 his opposition demonstrates the broad, legitimate application of the EAR encryption provisions. See
7 Exhibit B to Bernstein Declaration in Opposition (Commerce Department's 2002 Report on Foreign
8 Policy Export Controls, Ch. 10 - Encryption). Among other things, the Commerce Department report
9 indicates that:

10 * Encryption export controls apply to "retail encryption commodities and software" which
11 may be exported after a technical review to any end-user, including foreign governments,
under a license exception, including financial related products for banks and financial
institutions. Id. at 92.

12 * In FY 2001, the Commerce Department received 983 requests for technical review
13 covering 1,553 controlled encryption products, including source code. Of these, nearly
80% were classified as "retail" encryption items. Id. at 95.

14 * Also in FY 2001, the Commerce Department reviewed 422 encryption items controlled
15 for anti-terrorism purposes from 233 classification requests. Id.

16 * Also in FY 2001, the government processed 241 license applications for encryption
17 items, and approved 243 applications valued at \$31.1 million, including exports of non-
retail items to government end-users.

18 The government's review of "retail" encryption hardware and software exports, exports of
19 financial-related products, and exports of "non-retail" encryption items to foreign governments, are
20 among the plainly legitimate sweep of the EAR that have nothing to do with plaintiff's activities. As the
21 Commerce Department's report further indicates, the government and industry work cooperatively "to
22 assist law enforcement, protect national security, ensure continued U.S. technological leadership, and
23

24 ^{15/} Bernstein is also wrong that standing for an as-applied claim is sufficient to raise an overbreadth
25 claim on behalf of third parties. See Pl. Opp. at 17. A plaintiff must have standing related to the alleged
26 third party interests at issue in an overbreadth claim. Secretary of State of Maryland v. Joseph H. Munson
27 Co., 467 U.S. 947, 958 (1984). See also Board of Trustees, S.U.N.Y. v. Fox, 492 U.S. 469, 484 (1989)
28 (where plaintiff has direct standing to bring an as-applied claim and standing to vindicate third party
interests, then he may bring both as-applied and overbreadth claims).

1 promote the privacy and security of U.S. firms and citizens engaged in electronic commerce." *Id.* at 95.
2 These are among the goals served by the notice and review requirements of the EAR provisions on
3 encryption exports. Bernstein presents a challenge to the EAR that pertains to his own purported
4 "academic" interests and does not concern the manner in which the EAR encryption provisions are
5 broadly applied to thousands of other exporters. Even assuming that Bernstein engages in "speech"
6 activities,^{16/} exports by commercial enterprises of retail encryption products, and non-retail encryption
7 items to foreign governments, hardly constitute speech activities. As such, even if Bernstein had a
8 meritorious as-applied claim, which defendants vigorously dispute, facial invalidation would not be
9 warranted in any event.

10 **3. Technology and Technical Assistance:** A last issue worth noting concerns the EAR
11 provisions on technology and technical assistance, as to which defendants make two major points.

12 First, there is no basis for *facial* invalidation of the technology regulations. As noted above,
13 Bernstein has demonstrated no standing to vindicate interests unrelated to his own, and the EAR has a
14 plainly legitimate sweep to export activities by U.S. industry. The Ninth Circuit's rulings in United
15 States v. Edler Industries, 579 F.2d 516 (9th Cir. 1978) and United States v. Posey, 864 F.2d 1487,
16 1496-97 (9th Cir. 1989) make clear that these provisions have a plainly legitimate sweep. In particular,
17 the court in Edler regarded prior technology controls as a law of general applicability not directed at the
18 content of speech – notwithstanding that particular applications to scientific information were
19 conceivable. Edler, 579 F.2d at 519, 520; see Def. Mem. at 23. Also, on their face, these provisions
20 exclude published information, academic discourse, fundamental research, and classroom instruction.
21 See 15 C.F.R. §§ 734.7, 734.8, 734.9. The wording of these exemptions reasonably indicates that
22 academic activities are not regulated and, as such, presents no facial vagueness concern. Grayned v. City
23 of Rockford, 408 U.S. 104, 108 (1972) ("[c]ondemned to the use of words, we can never expect
24 mathematical certainty from our language"); see Def. Mem. at 24. The focus of the technology/technical
25 assistance provisions is the export of proprietary information used to assist in the manufacture of items
26 on the Commerce Control List. See 15 C.F.R. Part 772 (definitions). Any alleged impermissible

27 _____
28 ^{16/} Again, the fact that Bernstein equips millions with software sharply undermines this assumption.

1 applications to scientific discourse must be addressed as-applied claims.

2 Second, as to any as-applied claim concerning the technology provisions, Bernstein either blurs
3 his concerns with the export notice provision for encryption software, or speculates as to how the
4 technology provisions might be applicable to his activities. The technology provisions are distinct from
5 the notice requirement on encryption software exports, and any application of that requirement should be
6 addressed separately. The government specifically advised Bernstein that *non-software* information
7 about encryption would not be subject to the EAR at all if it did not meet the definition of "technology,"
8 and that, even if the information were "technology" under the EAR, it likewise would not be subject to
9 the EAR if it were publicly available (e.g., on the Internet). See Third Advisory Opinion at 3, ¶ (4) (Tab
10 5 to First Kritzer Declaration). The government also advised Bernstein that the EAR does not preclude
11 him from teaching or discussing encryption in an academic setting, either inside or outside the United
12 States, regardless of whether foreign persons are present or participating. Id. Invalidation of the EAR
13 technology provisions, on their face or as-applied, would be unfounded.

14 CONCLUSION

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

17 Respectfully Submitted,

18 ROBERT D. McCALLUM Jr.
19 Assistant Attorney General

20 DAVID W. SHAPIRO
21 United States Attorney

22 JOCELYN BURTON
23 California Bar No. 135879
24 Assistant United States Attorney
25 450 Golden Gate Avenue
26 San Francisco, California 94102
27 Telephone: (415) 436-7198
28

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 30, 2002, the foregoing Defendants' Reply to Plaintiff's Opposition to Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment was served by overnight express mail on:

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

ANTHONY J. COPPOLINO