Govt. Emergency Stay Motion, Sept. 10, 1997 in Bernstein v. Commerce

This is a series of page images from a fax machine.

If you want to view or print this document in pieces, here are the first ten pages, second ten pages, and final pages . You can also download the individual image files, named "page01.gif", "page02.gif", etc. (01 through 26).

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DANIEL J. BERNSTEIN,	)	
Plaintiff-Appellee,	)	
v.	)	No. _____
DEPARTMENT OF COMMERCE et al.,	)	(D.C. No. C-95-0582 MHP)
Defendants-Appellants.	)	

EMERGENCY MOTION UNDER CIRCUIT RULE 27-3

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

STEVEN W. PRESTON
Deputy Assistant Attorney General

DOUGLAS N. LETTER
SCOTT R. McINTOSH
Attorneys, Appellate Staff
Room 3127, Civil Division
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

CIRCUIT RULE 27-3 CERTIFICATE

1. The telephone numbers and office addresses of the attorneys for the parties are as follows:

Counsel for Defendants-Appellants:
Douglas N. Letter
Scott R. McIntosh
Room 3127, Civil Division
Department of Justice
950 Pennsylvania Avenue NW
Washington DC 20530
Tel: 202-514-4052 (Mr. McIntosh)
202-514-3602 (Mr. Letter)
Fax: 202-514-9405

Counsel for Plaintiff-Appellee:
Cindy A. Cohn
McGlashan & Sarrail
177 Bovet Road, Sixth Floor
San Mateo CA 94402
Tel: 415-341-2585
Fax: 415-341-1395

2. This motion requests (i) a stay of a district court injunction pending appeal and (ii) an immediate temporary stay of the injunction while the Court considers the underlying stay request. As explained more fully in the body of this motion, the district court's injunction presently permits the plaintiff-appellee to engage in immediate, unrestricted export of cryptographic software whose unlicensed export is prohibited by federal law for national security and foreign policy reasons. The appellee intends, inter alia, to place this software on the Internet, a step that will make the software available almost instantaneously around the world. Immediate relief from this Court, in the form of a temporary stay while the Court considers the government's underlying stay request, is necessary to preserve the status quo.

3. Ms. Cindy Cohn, lead counsel for the appellee, was notified yesterday of the impending filing of this motion. A copy of this motion is being transmitted to Ms. Cohn and Ms. Cohn's co-counsel by fax at the same time that the motion is being delivered to this Court.

by MB Watts
Scott R. McIntosh

Scott R. McIntosh
Counsel for Defendants-Appellants

INTRODUCTION

The Department of Commerce hereby moves, pursuant to Circuit Rule 27-3 and FRAP 8, for an emergency stay pending appeal. For reasons of national security and foreign policy, the President of the United States has directed the Department to restrict the export of encryption products — products, including computer software, that "scramble" messages so they cannot be understood by persons other than the sender and the intended recipient. On August 25, 1997, the District Court for the Northern District of California held that the Department's regulations restricting the export of encryption software are facially unconstitutional under the First Amendment. On the basis of that holding, the district court enjoined the government from enforcing these regulations against the plaintiff and other persons who wish to use the plaintiff's encryption software.

On September 9, 1997, the district court entered an order granting a partial stay of its injunction pending appeal. However, the court declined to stay the injunction with respect to particular encryption software that the plaintiff wishes to export, including updated versions of the software whose encryption capabilities are unknown and have not been reviewed by the government. In the absence of a full stay, the plaintiff will be able to distribute this encryption software overseas, immediately and irretrievably, before this Court has had an opportunity to review the district court's novel First Amendment ruling. The Department of Commerce requests a full stay pending appeal in order to preserve the status quo while this Court resolves the important questions posed by the district court's invalidation of the Department's export regulations. The Department further requests an

immediate temporary stay while the Court considers the Department's underlying stay request.

STATEMENT OF THE CASE

1. The national security of the United States depends in part on the ability of the government to obtain timely information about the activities and plans of potentially hostile foreign governments, groups, and individuals abroad. The United States therefore uses a variety of means to monitor and intercept communications by foreign intelligence targets. Among other things, the United States engages in signals intelligence ("SIGINT"), the collection and analysis of information from foreign electromagnetic signals. Declaration of William P. Crowell ("Crowell Dec.") ¶¶ 1-2 (copy attached). Primary responsibility for the government's SIGINT activities belongs to the National Security Agency ("NSA"), a component of the Department of Defense. Id. at ¶ 1.

The SIGINT capabilities of the United States are impaired by the use of encryption. Crowell Dec.¶ ¶ 3-4. Encryption is the process of converting a message from its original form (known as "plaintext") into a scrambled form (known as "ciphertext") that cannot be deciphered by persons other than the message's sender and its intended recipients. Id. ¶ 3 & n.1. Encryption can be performed by mechanical devices, like the famed "Enigma" machine used by Germany during the Second World War, or by electronic circuitry. Encryption also can be accomplished by computer software, which enables general-purpose computers to encrypt and decrypt electronic messages and other data.

Encryption has long been a tool in the conduct of military and foreign affairs. See, e.g., David Kahn, The Code Breakers: The Story of Secret Writing (1967). Today, foreign intelligence targets use encryption in an effort to maintain the secrecy of their communications. Crowell Dec. ¶¶ 3-4. For this reason, one of the NSA's principal SIGINT activities is cryptanalysis, the science of "reading" ciphertext without having access to the key that was used to encrypt the message. Id. ¶ 3. How readily ciphertext can be read through cryptanalysis depends, in large part, on the strength of the particular cryptographic algorithm used to encode the plaintext. The stronger the algorithm, the greater the odds that the ciphertext cannot be read at all or that the process of deciphering the message will take prohibitive amounts of time and effort.

2. The United States imposes legal restrictions on the export of a wide variety of products whose use abroad could compromise this country's national security and foreign policy interests. Because encryption can be used by foreign intelligence targets to deny the United States access to information vital to our national security interests, encryption products have long been included in these export restrictions.

Until recently, primary regulatory responsibility over the export of cryptographic products was vested in the Department of State. Acting pursuant to the Arms Export Control Act (AECA), 22 U.S.C. §§ 2751 et seq., and the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130, the Department of State regulates the export of "defense articles" and "defense services." Generally speaking, defense articles and services cannot

be exported without a license from the Department of State. With specified exceptions, cryptographic products were classified as "defense articles" under the ITAR and therefore could not be exported without a license.

In November 1996, President Clinton issued an Executive Order and Presidential memorandum transferring regulatory authority over the export of most encryption products, including the encryption software at issue in this case, from the Department of State to the Department of Commerce. Executive Order 13206, 61 Fed. Reg. 58767 (Nov. 19, 1996); 32 Weekly Comp. Pres. Doc. 2397 (Nov. 15, 1996) (memorandum). The Department of Commerce is responsible for administering the Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774, which regulate the export of so-called "dual use" items — items that have both military and civilian uses. See 15 C.F.R. § 730.3. At the heart of the EAR is the Commerce Control List (CCL), 15 C.F.R. Part 774, which lists the categories of items whose export is regulated under the EAR. Items listed on the CCL generally may not be exported without a license from the Department of Commerce's Bureau of Export Administration.

Acting pursuant to the President's directions, the Department of Commerce amended the CCL in December 1996 to cover encryption items transferred from the Department of State's regulatory jurisdiction. The Department also made a number of related amendments

to the EAR to carry out the terms of the President's Executive Order and Presidential memorandum. See generally 61 Fed. Reg. 68572-87 (Dec. 30, 1996).[1]

As amended, the CCL covers encryption commodities (i.e., hardware), encryption software, and encryption technology. 15 C.F.R. 742.15.[2] Because these items "may be used by persons abroad to harm national security, foreign policy and law enforcement interests," they generally may not be exported without a license. Ibid. Applications for licenses to export encryption items generally are reviewed on a case-by-case basis by the Bureau of Export Administration, in conjunction with other agencies, to determine whether the export is consistent with national security and foreign policy interests. Id. § 742.15(b); see also id. § 742.15(b)(4)(ii).[3]

Encryption software, like other software, may take either of two forms: "source code" or "object code." Source code is a set of instructions to a computer written in a programming language, such as "C" or BASIC, that can be read and understood by programmers and computer scientists. Crowell Dec. ¶ 5. Object code is a set of instructions in binary form ("zeroes" and "ones") that can be directly executed by a computer. Ibid. Source code can

---

[1] All citations to the EAR in this motion reflect the amendments in the foregoing Federal Register notice. Not all of those amendments have yet been reproduced in the Code of Federal Regulations.

[2] Each item on the CCL is assigned an Export Control Classification Number (ECCN). See 15 C.F.R. Part 772. Encryption commodities, software, and technology are listed as ECCN 5A002, 5D002, and 5E002, respectively. See 15 C.F.R. Part 774, Supplement 1.

[3] Certain encryption items are subject to less restrictive licensing rules and policies. See 15 C.F.R. § 742.15(b)(1)-(3). This case does not involve such items.

be converted automatically into object code through the use of commonly available computer programs called compilers. Ibid. When encryption source code is converted into object code in this fashion, it can be used to encrypt and decrypt messages and other data.

The EAR's restrictions on the export of encryption software apply both to source code and to object code. See 15 C.F.R. Part 772 (definition of "encryption software"). In his Executive Order and Presidential memorandum (see p. 4 supra), the President specified that encryption source code is subject to export control because of its functional capability to encrypt communications, not because of any information that the source code itself might convey to persons who are familiar with the programming language in which it is written. 32 Weekly Comp. Pres. Doc. 2398, ¶ 4 (Nov. 15, 1996); Executive Order 13026, § 1(c), 61 Fed. Reg. 58768 (Nov. 19, 1996). Accordingly, for export licensing purposes, encryption source code (and object code) are treated in the same manner as encryption hardware. See 15 C.F.R. Part 774, Supplement 1, ECCN 5D002 (Note). The export controls applicable to encryption software are correspondingly distinct from those generally applicable to other kinds of software. See id. § 742.15; see also id. Part 772 (definition of "commodity"). For example, while publicly available software is generally not subject to the EAR, the public availability exclusion does not apply to encryption software. See id. §§ 734.3(b)(3), 734.7-734.9.

In some circumstances, the availability and scope of export licenses under the EAR is affected by existing foreign availability of comparable items. See 15 C.F.R. Part 768. However, in his Executive Order, the President determined that the export of encryption

items "could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States." Executive Order 13206, § 1(a), 61 Fed. Reg. 58767 (Nov. 19, 1996). The President further determined that "facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure or judicial review without revealing or implicating classified information that could harm United States national security and foreign policy interests." Ibid. The President therefore directed that the provisions of the EAR relating to foreign availability shall not apply to encryption items. Ibid.; see 15 C.F.R. § 768.1(b).

3. This case involves a facial challenge to the constitutionality of the foregoing restrictions on the export of encryption software. The plaintiff, Daniel Bernstein, is a professor and a computer programmer. As a graduate student, Bernstein created a computer program called "Snuffle" that is designed to encrypt and decrypt text messages interactively. Bernstein has stated that he wishes, inter alia, to distribute Snuffle to other persons over the Internet. Because of the global nature of the Internet, circulation of Snuffle in the manner desired by Bernstein would entail the immediate and unrestricted distribution of Snuffle abroad.

In 1992, Bernstein approached the Department of State to inquire about the status of Snuffle and related explanatory materials under the export regulations then in effect (see pp. 3-4 supra). After a lengthy series of exchanges, Bernstein ultimately was informed that the source code for Snuffle could not be exported without a license, but that a license would not

be required to export the other materials in question. See Bernstein v. Department of State, 922 F. Supp. 1426, 1430, 1433-34 (N.D. Cal. 1996) (Bernstein I); Bernstein v. Department of State, 945 F. Supp. 1279, 1284 (N.D. Cal. 1996) (Bernstein II).[4]

Bernstein did not apply for an export license. Instead, he filed suit against the Department of State in 1995 to challenge the constitutionality of the then-existing restrictions on the export of encryption software and related restrictions on the export of "technical data" relating to encryption products. Bernstein advanced a variety of First Amendment and other constitutional claims. For present purposes, the most pertinent constitutional claim was a claim that the restrictions on encryption software exports were facially invalid under the First Amendment as an unconstitutional prior restraint.

The Department of State moved to dismiss Bernstein's constitutional claims on the ground that the claims were not colorable and therefore were nonjusticiable. With respect to the First Amendment, the Department asserted, inter alia, that the appropriate analytic framework is supplied by United States v. O'Brien, 391 U.S. 367 (1968). Under O'Brien and its progeny, "a content-neutral [law] will be sustained [under the First Amendment] if 'it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restrictions on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.'"

---

[4] The Department of State advised Bernstein that a license would be required for the export of two supporting documents if, but only if, the purpose of the export were to assist a foreign person in obtaining or developing Snuffle itself. See Bernstein II, 945 F. Supp. at 1284.

Turner Broadcasting System, Inc. v. FCC, 114 S. Ct. 2445, 2469 (1994) (quoting O'Brien, 391 U.S. at 377). The Department contended that the challenged export restrictions are governed by O'Brien because they are directed not at the informational content (if any) of encryption source code, but instead at the functional capacity of encryption source code (like other encryption items) to encrypt communications and thereby impede the government's foreign intelligence capabilities.

In April 1996, the district court (Patel, J.) denied the government's motion to dismiss, ruling that Bernstein's First Amendment claims were colorable and therefore justiciable. The district court held that computer source code is "speech" for First Amendment purposes. Bernstein I, 922 F. Supp. at 1434-36. The district court further held, inter alia, that Bernstein's prior restraint claim was a colorable one. Id. at 1437-38. In so holding, the district court analogized the licensing of encryption software exports to the prior restraints at issue in New York Times v. United States, 403 U.S. 713 (1970) (per curiam) (the Pentagon Papers case), and Near v. Minnesota, 283 U.S. 697 (1931). See id. at 1438.

In December 1996, shortly before the transfer of regulatory jurisdiction from the Department of State to the Department of Commerce (see p. 4 supra), the district court issued an order granting partial summary judgment in favor of Bernstein. In relevant part, the district court held that the licensing requirements for the export of encryption software were facially invalid as a prior restraint on First Amendment speech. Bernstein II, 945 F. Supp. at 1286-90. For purposes of its decision, the district court accepted the government's contention that the regulatory purposes behind the licensing requirements are content-

neutral. Id. at 1289. However, the court held that the licensing requirements were nonetheless facially invalid because they lacked the procedural safeguards that the Supreme Court has required for the licensing of parades, marches, and similar expressive activities. Id. at 1289-90. The district court confined its order to declaratory relief, denying a motion by Bernstein for a preliminary injunction relating to his classroom teaching activities because the challenged regulations did not require a license for those activities. Id. at 1296.

4. Following the transfer of regulatory jurisdiction to the Department of Commerce and the accompanying amendments to the EAR, Bernstein filed an amended complaint, adding the Department of Commerce and other agencies as defendants and advancing the same constitutional objections (as well as new statutory objections) to the new regulations. The parties thereafter filed renewed cross-motions for summary judgment.

On August 25, 1997, the district court issued a memorandum order (copy attached) disposing of the summary judgment motions. The district court rejected Bernstein's new statutory claims, but it held that the Department of Commerce's restrictions on the export of encryption software are a facially invalid prior restraint, for essentially the same reasons that the court had previously struck down the Department of State's corresponding regulations. Mem. 22-28. In so holding, the district court acknowledged that the constitutional issues addressed in its decision "are novel, complex, and of public importance * * * ." Id. at 30. In light of the transfer of regulatory jurisdiction to the Department of Commerce, the court dismissed all other agencies named in the amended complaint.

As part of its memorandum order, the district court entered a permanent injunction against the Department of Commerce. The injunction prohibits the Department from enforcing or applying the invalidated regulatory provisions "with respect to [Bernstein] or anyone who uses, discusses, or publishes or seeks to use, discuss or publish [Bernstein's] encryption program and related materials * * * ." Mem. 31-32. The injunction further prohibit the Department from "interfering with [Bernstein] or any other person described in [the foregoing sentence] in the exercise of their federal constitutional rights as declared in this order." Id. at 32.

The Department of Commerce promptly moved for a stay of the district court's injunction pending appeal. On September 9, 1997, the district court entered an order (copy attached) staying the injunction in part but not in whole.[5] The district court stayed its injunction with respect to persons other than Bernstein and encryption programs other than Snuffle. However, the district court declined to stay the injunction with respect to Bernstein's export of Snuffle, either in its current form or in updated forms. As a consequence, the district court's injunction permits Bernstein to export existing and updated versions of Snuffle to any persons and by any means, including via the Internet, during the pendency of the Department's appeal. The district court denied an oral request by the

[5] The district court earlier issued a temporary oral stay that remained in effect until the entry of the written stay order on September 9.

Department to stay its injunction temporarily for 24 hours while this motion is presented to this Court.[6]

ARGUMENT

The District Court's Injunction Should Be Stayed In Its Entirety Pending Appeal

In granting a partial stay of its injunction pending appeal, the district court took a limited step toward preserving the status quo while its novel First Amendment ruling is under review in this Court. The court abused its discretion, however, in excluding Bernstein's export of existing and updated versions of Snuffle — the very software that precipitated this litigation — from the scope of its stay.

The availability of a stay pending appeal turns on two interrelated legal tests, which represent "the outer reaches of a single continuum." Artukovic v. Rison, 784 F.2d 1354, 1355 (9th Cir. 1986). "At one end of the continuum, the moving party is required to show both a probability of success on the merits and the possibility of irreparable injury." Lopez v. Heckler, 713 F.2d 1432, 1435 (9th Cir.), rev'd on other grounds, 463 U.S. 1328 (1983). "At the other end of the continuum, the moving party must demonstrate that serious legal questions are raised and that the balance of hardships tips sharply in its favor." Ibid. "'[T]he relative hardship to the parties' is the 'critical element' in deciding at which point along the continuum a stay is justified." Ibid. In addition, when an injunction restricts the

---

[6] The district court signed the partial stay order at the conclusion of a telephonic hearing on September 9. The court directed that a transcript of the hearing be deemed a part of the stay order. The transcript of the district court's remarks will be submitted to this Court as soon as it is available.

government's power to carry out an important regulatory program, as it does in this case, "the public interest is a factor to be strongly considered." Ibid.

Under these standards, the Department of Commerce is entitled to a full stay of the district court's injunction pending appeal. The district court's unprecedented holding that the government's restrictions on the export of cryptographic software are a facially unconstitutional prior restraint is likely to be reversed on appeal, and in all events is sufficiently novel and debatable that "serious legal questions" exist about its correctness. At the same time, the balance of harms and the public interest weigh decisively in favor of preserving the status quo while this Court reviews the district court's First Amendment ruling. The government therefore asks this Court: (1) to stay the district court's injunction in its entirety pending appeal; and (2) to issue an immediate temporary stay while the underlying stay request is under consideration. These grounds for relief were before the district court when it declined to grant a full stay pending appeal.

I. The District Court's First Amendment Ruling Is Likely To Be Reversed

The heart of the district court's decision is its holding that the government's longstanding restrictions on the export of encryption software amount to a facially unconstitutional prior restraint on First Amendment speech. It can hardly be gainsaid that this holding raises "serious legal questions" (Lopez, 713 F.2d at 1435). Indeed, in the course of framing its injunction, the district court itself acknowledged that the legal issues underlying its decision are "novel [and] complex." Mem. 30. The district court's unprecedented holding is sufficiently at odds with settled First Amendment principles that it is likely to be reversed on appeal.

A. It should be evident from the outset that the regulatory scheme invalidated by the district court bears no meaningful resemblance to the classic kinds of prior restraint at issue in cases like New York Times v. United States, 403 U.S. 713 (1976) (per curiam), and Near v. Minnesota, 283 U.S. 697 (1931), on which the district court has relied. In New York Times, the government sought to enjoin the publication of the Pentagon Papers because the government feared that the documents contained "'information whose disclosure would endanger the national security.'" 403 U.S. at 718 (Black, J., concurring) (quoting government brief); id. at 726 n.* (Brennan, J., concurring). Similarly, in Near, state officials sought to censor a newspaper by enjoining it from publishing "scandalous and defamatory matter," including "charges of official misconduct." 283 U.S. at 711. In these and other conventional prior restraint cases, the government's underlying object was to prevent speakers from

communicating disfavored information and ideas to the public. The prior restraints thus went to the core of the First Amendment, which serves first and foremost to preserve the free flow of information and ideas. It is largely for this reason that the use of prior restraints is subject to a "heavy presumption" (New York Times, 403 U.S. at 714) of unconstitutionality.

Here, in contrast, the government's restrictions on the export of cryptographic software are manifestly not aimed at preventing the free exchange of information and ideas. The President's Executive Order expressly provides that the export of cryptographic software is controlled "because of such software's functional capacity" — that is, its ability to encrypt data — "rather than because of any possible informational value of such software * * *." Executive Order 13026, § 1(a), 61 Fed. Reg. 58767 (Nov. 19, 1996). The applicable provisions of the EAR rest on the same principle. See, e.g., 15 C.F.R. Part 772 (definition of "commodity"). It is for this reason that the EAR subjects the export of encryption software to the same controls that apply to encryption hardware, the export which cannot even arguably be characterized as a form of "speech." See, e.g., id. § 742.15.

It is undeniably true that encryption source code, such as the source code for Snuffle attached to this motion, can be read and understood by computer scientists and programmers.[7] It is equally true, however, that source code is routinely written, distributed, and used for the wholly non-expressive purpose of making a computer carry out a particular

[7] In contrast, object code (see p. 5 supra) is a sequence of binary characters ("0s" and "1s") that cannot be read or understood by humans and cannot be used in any meaningful way to communicate cryptographic information or ideas.

task. As the parties have stipulated in this case, "[c]ryptographic 'source code' is a computer program written in a computer language * * * that can be used to encrypt and decrypt information." Joint Statement of Undisputed Facts ¶ 6 (Sept. 20, 1996) (emphasis added). The regulatory provisions that the district court has condemned as an unconstitutional prior restraint are directed at this non-expressive function of cryptographic software, not at whatever information may be claimed to be embodied and conveyed in a particular case by source code itself.

B. As the district court pointed out, when a discretionary licensing scheme encompasses expressive activities, it may present the censorship risks associated with traditional prior restraints even if the underlying object of the scheme is unrelated to the suppression of speech. See, e.g., City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750 (1988); FW/PBS, Inc. v. City of Dallas, 493 U.S. 215 (1990). It does not follow, however, that all discretionary licensing schemes are subject to the kind of facial invalidation that Bernstein has sought and the district court has granted in this case. Licensing schemes are subject to facial challenge under the First Amendment only in certain circumstances, and those circumstances are not present here.

The Supreme Court's decision in Lakewood sets out the standards for "distinguish[ing] [licensing] laws that are vulnerable to facial challenge [under the First Amendment] from those that are not." 486 U.S. at 759. In order for a licensing law to be subject to a facial challenge, it "must have a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat" of censorship. Ibid. In

contrast, "laws of general application that are not aimed at conduct commonly associated with expression and do not permit licensing determinations to be made on the basis of ongoing expression or the words about to be spoken" are not subject to facial invalidation. Id. at 760-61. Thus, for example, a law requiring building permits is not subject to facial challenge on prior restraint grounds, even if it applies in some cases to conduct associated with speech (such as the construction of a newspaper printing plant) and could be used in a particular case for the purpose of restraining speech or expressive conduct. Id. at 762.

In Roulette v. City of Seattle, 97 F.3d 300 (9th Cir. 1996), this Court recently reiterated the narrowness of the circumstances in which government regulations may be facially invalidated on First Amendment grounds. In Roulette, the Court rejected a facial challenge to a Seattle ordinance that restricted people from sitting on sidewalks. The Court acknowledged that sitting on sidewalks can be undertaken for expressive purposes. 97 F.3d at 303. However, the Court held that government regulations are subject to facial invalidation under the First Amendment only when they are directed at activities that are "integral to, or commonly associated with, expression." Id. at 304, 305. Quoting Lakewood, the Court emphasized that "a facial freedom of speech attack must fail unless, at a minimum, the challenged statute 'is directed narrowly and specifically at expression or conduct commonly associated with expression.'" Id. at 305 (quoting Lakewood, 486 U.S. at 760).

Applying these standards, the district court erred in entertaining and approving a facial First Amendment challenge in this case. The EAR is a "law[] of general application that [is] not aimed at conduct commonly associated with expression * * * ." Lakewood, 486 U.S. at

760-61. It applies to the export of a vast range of "dual use" items, including but in no way limited to encryption items. See generally 15 C.F.R. Part 774, Supplement 1. [8] Neither the EAR as a whole nor its provisions governing encryption items are "'directed narrowly and specifically at expression or conduct commonly associated with expression.'" Roulette, 97 F.3d at 305. At most, it may be said that this general licensing scheme covers activities, such as the export of encryption source code, that theoretically could (but need not) be undertaken in some instances for expressive purposes. See Mem 23. But it does not follow the licensing scheme is therefore subject to facial invalidation as an unconstitutional prior restraint, any more than a building permit regulation is subject to facial invalidation merely because it encompasses potentially expressive activities such as the construction of a printing plant. See Lakewood, 486 U.S. at 305. The district court's insistence that "[t]he encryption regulations * * * [are] specifically directed at speech protected by the First Amendment" (Mem 24) is an ipse dixit that simply disregards the breadth, generality, and purpose of the licensing regime.

As the district court noted (Mem. 24), the EAR treats encryption software differently from, and in certain respects more restrictively than, other kinds of software listed on the CCL. See pp. 6-7 supra. But this differential treatment does not support the facial invalidation of the EAR's encryption software provisions. As explained above, the EAR

---

[8] For example, the EAR covers such items as reactor and power plant simulators (ECCN 0B008); specified human pathogens and toxins (ECCN 1C351); equipment relating to nuclear material handling and processing (ECCN 2A291); and "radiation hardened" integrated circuits (ECCN 3A001.a.1). See 15 C.F.R. Part 774, Supplement 1.

subjects encryption software to different restrictions precisely because the government is not concerned with the potential informational content of such software, but rather with its non-expressive capability to make a computer encrypt data. To hold that the government is impermissibly "singling out" encryption software by declining to regulate it on the basis of its potential informational value is to turn the logic of the prior restraint doctrine on its head.

II. The Balance of Harms and the Public Interest Strongly Favor a Full Stay Pending Appeal

As the foregoing discussion shows, there is a substantial prospect that the district court's novel First Amendment ruling in this case will be reversed on appeal. At the same time, the balance of harms and the public interest weigh strongly in favor of preserving the status quo by staying the district court's injunction in its entirety pending appeal.

A. As explained above, the federal government restricts the export of encryption items, including but not limited to encryption software, for important reasons of national security and foreign policy. The President has expressly determined that "[e]ncryption products, when used outside the United States, can jeopardize our foreign policy and national security interests" and "can threaten the safety of U.S. citizens here and abroad * * *." 32 Weekly Comp. Pres. Doc. 2397 (Nov. 15, 1996). The use of encryption products by foreign intelligence targets can impede the intelligence-gathering capabilities of the United States and thereby compromise the ability of the President and other government officials to anticipate and respond to foreign threats in a timely and effective manner. The encryption

provisions of the EAR reflect the considered judgment of the President that the unrestricted export of encryption products poses a genuine threat to our national interests.

By declining to enter a full stay pending appeal, the district court has opened the door for Bernstein to engage in the immediate and unrestricted export of the very kind of software product that the President has found it necessary for the Department of Commerce to regulate under the EAR. Snuffle is designed to "direct [a] computer to transform information into ciphertext and back into plain text again," including encrypting and decrypting text exchanges interactively. Joint Statement of Undisputed Facts ¶ 11 (Sept. 20, 1996). The district court's injunction allows Bernstein to export this cryptographic software by any means, in any quantity, to any person in the world. Moreover, the district court has permitted Bernstein not only to export Snuffle in its current form, but also to export updated versions of Snuffle whose encryption capabilities potentially could be even greater. See Declaration of William A. Reinsch ("Reinsch Dec.") ¶ 7 (copy attached).

Although Bernstein's stated reasons for wishing to distribute his Snuffle source code over the Internet may be academic ones, the district court has not confined Bernstein to exporting Snuffle for academic purposes. Under the terms of the injunction, Bernstein may export Snuffle for any reason, including commercial or other purposes if he so chooses. More important, even if Bernstein himself distributes Snuffle abroad solely for academic purposes, neither Bernstein nor the courts have any way to limit the uses to which Snuffle may be put once it has been distributed. For example, Bernstein has stated his intention to post the source code for Snuffle on an Internet "newsgroup," an electronic forum that

distributes postings automatically around the world and is accessible to any person with Internet access. See Reno v. ACLU, 117 S. Ct. 2329, 2335, 2349 (1997) (Internet newsgroups and the World Wide Web are "open to all comers"). Once Snuffle is exported to a person or group abroad, whether via the Internet or in some other way, it is impossible to control either the persons who receive it or the use that they make of it.

We note that, at some point in the past, copies of the source code for Snuffle were exported abroad by unknown persons, in apparent violation of federal export laws, and those copies are currently available for downloading from several publicly accessible computers overseas. Reinsch Dec. ¶ 8. However, the availability of copies of Snuffle on these foreign computers in no way eliminates the risk of irreparable injury posed by the district court's injunction. Absent a full stay pending appeal, Bernstein readily can bring about far wider and more indiscriminate distribution and use of Snuffle than has occurred already -- for example, by posting Snuffle on Internet newsgroups and the World Wide Web and/or by engaging in other forms of direct distribution to interested users overseas. Ibid. Moreover, the district court's injunction permits Bernstein to distribute not only the current version of Snuffle, but also updated versions that are not now available abroad and whose capabilities could well exceed those of Snuffle in its current form.[9] See Crowell Dec. ¶¶ 8-9.

B. In contrast to the risks that the denial of a full stay would pose, the granting of a full stay will not materially prejudice Bernstein's interests. A full stay will simply preserve

---

[9] A stay pending appeal would thus remain imperative even if the source code for the existing version of Snuffle were posted on the Internet.

the status quo by preventing the unrestricted export of the Snuffle program. Bernstein will remain free, as he has been throughout this litigation, to engage in academic discussions of the cryptographic ideas and algorithms underlying Snuffle or any other encryption program. Crowell Dec. ¶ 10.[10] A stay therefore will not materially compromise Bernstein's ability to engage in academic dialogue.

To minimize any possible adverse impact on Bernstein, this appeal can be briefed and argued on an expedited basis. For example, the appeal could be fully briefed and ready for calendaring within two months and could be argued and taken under submission at the Court's first available sitting thereafter. Given the length of time that the parties have already been engaged in this litigation, the brief additional delay involved in this kind of expedited appeal can hardly be said to impose a significant burden on Bernstein.

---

[10] The EAR's encryption provisions prohibit the unlicensed provision of "technical assistance" to foreign persons with the intent to aid a foreign person in the development or manufacture abroad of encryption commodities or software that would be controlled under the EAR. See 15 C.F.R. § 744.9(a). However, "the mere teaching or discussion of information about cryptography, including, for example, in an academic setting, by itself [does] not establish the intent described in this section, even where foreign persons are present." Ibid.

CONCLUSION

For the foregoing reasons, this Court should: (1) issue an immediate temporary stay of the injunction set forth in the district court's memorandum order of August 25, 1997; and (2) thereafter issue a full stay of the injunction pending expedited appeal.

Respectfully submitted,

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

STEVEN W. PRESTON
Deputy Assistant Attorney General

by MB Matte
Douglas N. Letter 9/9/97
DOUGLAS N. LETTER

by MB Matte
Scott R. McIntosh 9/9/97
SCOTT R. McINTOSH

Attorneys, Appellate Staff
Room 3127, Civil Division
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
(202) 514-4052