Govt. Appeal Brief, October 16, 1997, in Bernstein v. Commerce

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

If you want to view or print it in pieces, here are the first ten pages, and next ten pages, and next ten pages, and next ten pages, and next ten pages, and next ten pages, and next ten pages, and remaining pages of the motion. You can also download the individual image files, named "page01.gif", "page02.gif", etc. (1 through 81).

NO. 97-16686

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DANIEL J. BERNSTEIN,

Plaintiff-Appellee,

v.

U.S. DEPARTMENT OF COMMERCE, et al.,

Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIEF FOR THE APPELLANTS

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

STEPHEN W. PRESTON
Deputy Assistant Attorney General

DOUGLAS N. LETTER
SCOTT R. McINTOSH
Attorneys, Appellate Staff
Civil Division, Room 9550
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530-0001

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

STATEMENT OF JURISDICTION 1

STATEMENT OF ISSUES 2

STATEMENT OF THE CASE 3

I. Nature of Case and Proceedings Below 3

II. Statement of Facts 4

A. Regulatory Background 4

B. The Present Litigation 14

SUMMARY OF ARGUMENT 19

ARGUMENT 23

I. THE EAR'S CONTROLS ON THE EXPORT OF ENCRYPTION SOURCE CODE DO NOT VIOLATE THE FIRST AMENDMENT 23

A. The EAR's Export Controls Are Constitutionally Permissible Content-Neutral Regulations 24

B. The EAR's Export Controls Are Not A Facially Unconstitutional Prior Restraint 36

II. THE DISTRICT COURT'S DECLARATORY AND INJUNCTIVE RELIEF IS TOO BROAD 44

A. Encryption Object Code and Encryption Commodities 45

B. Encryption Technology 47

CONCLUSION 53

STATEMENT OF RELATED CASES

ADDENDUM

CERTIFICATE OF COMPLIANCE

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

Cases Page

Bateman v. Mnemonics, Inc., 79 F.3d 1532 (11th Cir. 1996) 6

Bennett v. Spear, 117 S. Ct. 1154 (1997) 48

Bernstein v. Department of State, 922 F. Supp. 1426
(N.D. Cal. 1996) .... passim

Bernstein v. Department of State, 945 F. Supp. 1279
(N.D. Cal. 1996) .... passim

Blount v. SEC, 61 F.3d 938 (D.C. Cir. 1995),
cert. denied, 116 S. Ct. 1351 (1996) 31

Brown Bag Software v. Symantec Corp., 960 F.2d 1465 (9th Cir.),
cert. denied, 506 U.S. 869 (1992) 7

Bullfrog Films, Inc. v. Wick, 847 F.2d 502 (9th Cir. 1988) 24

Cadence Design Systems, Inc. v. Avant! Corp., 1997 WL 583702
(9th Cir. Sept. 23, 1997) 7

Carreras v. City of Anaheim, 768 F.2d 1039 (9th Cir. 1985) 43

City of Lakewood v. Plain Dealer Publishing Co.,
486 U.S. 750 (1988) 21,39,40,41,42

Desert Outdoor Advertising, Inc. v. City of Moreno Valley,
103 F.3d 814 (9th Cir. 1996), cert. denied, 65 U.S.L.W. 3666
(Oct. 14, 1997) 43

Digidyne Corp. v. Data General Corp., 734 F.2d 1336 (9th Cir. 1984), cert. denied, 473 U.S. 908 (1985) 6

FW/PBS, Inc. v. City of Dallas, 493 U.S. 215 (1990) 43

Forsyth County v. Nationalist Movement, 505 U.S. 123 (1992) 43

Gaudiya Vaishnava Society v. City and County of San Francisco, 952 F.2d 1059 (9th Cir. 1990), cert. denied, 504 U.S. 914 (1992) 43

Gerritson v. City of Los Angeles, 994 F.2d 570 (9th Cir.), cert. denied, 510 U.S. 915 (1993) 43

Grossman v. City of Portland, 33 F.3d 1200 (9th Cir. 1994) 43

Haig v. Agee, 453 U.S. 280 (1981) 24,32

Home Box Office, Inc. v. FCC, 567 F.2d 9 (D.C. Cir.), cert. denied, 434 U.S. 829 (1977) 31

ISC-Bunker Ramo Corp. v. Altech, Inc., 765 F. Supp. 1310 (N.D. Ill. 1990) 45

Information Providers' Coalition v. FCC, 928 F.2d 866 (9th Cir. 1991) . 23

International Brotherhood of Teamsters v. Department of Transportation, 932 F.2d 1292 (9th Cir. 1991) 23

Johnson Controls, Inc. v. Phoenix Control Systems, Inc., 886 F.2d 1173 (9th Cir. 1989) 7

Karn v. U.S. Department of State, 925 F. Supp. 1 (D.D.C. 1996), remanded, 107 F.3d 923 (D.C. Cir. 1997) 8

Kev, Inc. v. Kitsap County, 793 F.2d 1053 (9th Cir. 1986) 25

Lovell v. Griffin, 303 U.S. 444 (1938) 43

Multnomah Legal Services Workers Union v. Legal Services Corp., 936 F.2d 1547 (9th Cir. 1991) 23

Near v. Minnesota, 283 U.S. 697 (1931) 16,37

New York Times v. United States, 403 U.S. 713 (1970) 16,21,37,38

One World One Family Now v. City and County of Honolulu, 76 F.3d 1009 (9th Cir.), cert. denied, 117 S. Ct. 554 (1996) 25

Rosen v. Port of Portland, 641 F.2d 1243 (9th Cir. 1981) 43

Roulette v. City of Seattle, 97 F.3d 300 (9th Cir. 1996) 40

Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1993) 7,45

Shuttlesworth v. City of Birmingham, 394 U.S. 147 (1969) 43

Sports Form, Inc. v. United Press International, Inc., 686 F.2d 750 (9th Cir. 1982) 23

Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622 (1994) . . . passim

United States v. Edler Industries, 579 F.2d 516 (9th Cir. 1978) . . 15,50,51

United States v. Posey, 864 F.2d 1487 (9th Cir. 1989) 51

Ward v. Rock Against Racism, 491 U.S. 781 (1989) 25,29,30,31,36

Statutes and Regulations

28 U.S.C. 1291 2

28 U.S.C. 1331 1

International Emergency Economic Powers Act,
50 U.S.C. 1701-1706 9

Export Administration Act of 1979, 50 U.S.C. App. 2401 et seq. 9

Export Administration Regulations, 15 C.F.R. 730-774 . . . . passim

15 C.F.R. 730.3 9
15 C.F.R. 732.2(b) 11,13
15 C.F.R. 734.2(b)(9)(i)(A)-(B) 13,51
15 C.F.R. 734.2(b)(9)(ii) 13
15 C.F.R. 734.3(b)(2) 30
15 C.F.R. 734.3(b)(3) 11,13,29,49
15 C.F.R. 734.3(b)(3)(i) 49
15 C.F.R. 734.7 11,29,49
15 C.F.R. 734.8 11,29,49
15 C.F.R. 734.9 11,29,49
15 C.F.R. 734.10 11
15 C.F.R. 736.2(b)(1) 9
15 C.F.R. 736.2(b)(2)-(10) 9
15 C.F.R. 738.2(d) 10
15 C.F.R. 738.2(d)(2)(i) 10
15 C.F.R. 740.9(c)(3) 13
15 C.F.R. 740.13(d)(2) 13
15 C.F.R. 742.15 12,13,29
15 C.F.R. 742.15(b) 36
15 C.F.R. 742.15(b)(1)-(3) 12
15 C.F.R. 744.9 50,51,52
15 C.F.R. 768 . . . .
15 C.F.R. 768.1(b) 14
15 C.F.R. 772 . . . . passim
15 C.F.R. 774 Supplement No. 1 (Commerce Control List) . . . . passim

International Traffic in Arms Regulations, 22 C.F.R. 120-130 8

Other Materials

Executive Order 12924, 59 Fed. Reg. 43437 (Aug. 23, 1994) 9

Executive Order 13206, 61 Fed. Reg. 58767 (Nov. 19, 1996) ..... passim

61 Fed. Reg. 68576 (Dec. 30, 1996) 9

62 Fed. Reg. 43629 (Aug. 13, 1997) 9

32 Weekly Comp. Pres. Doc. 2397 (Nov. 15, 1996) 9,12,13,26

David Kahn, The Code Breakers: The Story of Secret Writing (1967) ... 5

John Hart Ely, Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis, 88 Harv. L. Rev. 1482 (1975) 31

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NO. 97-16686

DANIEL J. BERNSTEIN,

Plaintiff-Appellee,

v.

U.S. DEPARTMENT OF COMMERCE, et al.,

Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIEF FOR THE APPELLANTS

STATEMENT OF JURISDICTION

1. This is a suit for declaratory and injunctive relief against the Department of Commerce and other federal agencies based on federal statutory and constitutional claims. The jurisdiction of the district court over the subject matter of the suit was asserted under 28 U.S.C. 1331.

2. The judgment under appeal is the final judgment of the district court. The order is within the appellate jurisdiction of this Court under 28 U.S.C. 1291.

3. The judgment of the district court was entered on August 25, 1997. The notice of appeal was filed on September 8, 1997, within the time permitted by Rule 4(a)(1) of the Federal Rules of Appellate Procedure.

STATEMENT OF ISSUES

The Export Administration Regulations (EAR), 15 C.F.R. 730-774 (1997), control the export of a variety of "dual use" products with potential military as well as commercial applications, including computer software and hardware that can be used to encrypt data. The issues presented are:

1. Whether the district court erred in holding that the EAR's controls on the export of encryption software are facially unconstitutional under the First Amendment.

2. Whether the district court erred in invalidating the EAR's controls on the export of encryption products other than software.

STATEMENT OF THE CASE

I. Nature of Case and Proceedings Below

The Department of Commerce is responsible for administering the Export Administration Regulations (EAR), which control the export of "dual use" products that can be used for military as well as civilian purposes. As part of this responsibility, the Department has been directed by the President of the United States to control the export of encryption products — products, including computer software, that can scramble electronic data to conceal their contents. The President has determined that the use of encryption products outside the United States can jeopardize this country's foreign policy and national security interests and can threaten the safety of American citizens here and abroad.

This case presents a challenge to the constitutionality of the EAR's controls on the export of encryption software. The plaintiff, Daniel Bernstein, is a professor who wishes to distribute encryption software programs around the world. He asserts that the EAR's controls on the export of encryption software violate the First Amendment. Bernstein brought this suit against the federal government in the District Court for the Northern District of California to enjoin the government from enforcing these and other encryption export controls.

On August 25, 1997, the district court (Patel, J.) issued a decision holding that the EAR's controls on the export of encryption software are a facially unconstitutional prior restraint on speech. On the basis of this holding, which the district court acknowledged to be "novel," the court issued a declaratory judgment invalidating all of the EAR's controls on the export of encryption products, including export controls on items other than software, and enjoined the Department of Commerce from enforcing the invalidated controls against Bernstein and anyone else who wishes to use Bernstein's encryption software. The government is appealing to contest both the merits of the district court's underlying First Amendment ruling and the breadth of the court's declaratory and injunctive relief.

II. Statement of Facts

A. Regulatory Background

The regulations at issue in this case are designed to protect the security of the United States by controlling the export of products whose use abroad could jeopardize our national security and foreign policy interests. To place Bernstein's constitutional challenge to these regulations in context, we first summarize basic facts regarding cryptography and encryption products, then describe the regulatory provisions that control the export of such products.

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. ER 96. Primary responsibility for the government's SIGINT activities belongs to the National Security Agency (NSA), a component of the Department of Defense. Ibid.

The SIGINT capabilities of the United States can be significantly compromised by the use of encryption by foreign intelligence targets. ER 96. Encryption is the process of converting a message from its original form (commonly known as "plaintext") into a scrambled form (known as "ciphertext") that cannot be deciphered by persons who lack the "key" needed to unscramble the message. Id. at 96 n.2.

Encryption has long been a tool in the conduct of military and foreign affairs. ER 97; see generally 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. ER 97. 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. at 96-97.

2. Until the end of the Second World War, encryption was ordinarily performed by mechanical devices, such as the "Enigma" machines used by Nazi Germany. Since then, mechanical encryption devices have been largely replaced with electronic ones. Today, messages can be encrypted electronically through the use of dedicated hardware, such as the electronic circuitry embedded in a telephone scrambler. In addition, encryption now can be performed by general-purpose computers, including "desktop" computers of the sort in common use here and abroad.

In order for a computer to encrypt data, it must use encryption software that controls the encoding of the data. Because the constitutional claims in this case focus on encryption software, as distinct from encryption hardware, a brief discussion of software is required before we turn to the regulations at issue.

A software program consists of "a set of instructions [to a computer] that allows the system to accomplish a particular task." Digidyne Corp. v. Data General Corp., 734 F.2d 1336, 1342 (9th Cir. 1984), cert. denied, 473 U.S. 908 (1985); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1537 n.11 (11th Cir. 1996) ("computer software is the set of instructions * * * that tell the hardware to perform certain tasks"). The instructions that make up a software program may represented either as "object code" or "source code." Object code represents the instructions as a sequence of binary digits (0s and 1s) that can be executed directly by the computer's microprocessor. Cadence Design Systems, Inc. v. Avant! Corp., 1997 WL 583702, *1 n.2 (9th Cir. Sept. 23, 1997); Johnson Controls, Inc. v. Phoenix Control Systems, Inc., 886 F.2d 1173, 1175 n.2 (9th Cir. 1989). Source code represents the same computer instructions in "specialized alphanumeric [programming] languages" such as BASIC, C, or Java. Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514 n.2 (9th Cir. 1993).

Source code can be read by persons who are trained in the particular programming language in which the source code is written. Brown Bag Software v. Symantec Corp., 960 F.2d 1465, 1468 n.1 (9th Cir.), cert. denied, 506 U.S. 869 (1992). However, it is not necessary to read source code — or even to be able to read it, for that matter — in order to use it to control the operation of a computer. Source code may be converted automatically into object code through the use of commonly available conversion software called a compiler. ER 101, 301; Sega Enterprises, 977 F.2d at 1514 n.2. As a result, software products distributed in the form of source code can be used to make computers perform desired tasks — in the case of encryption source code, the task of encrypting data.

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

Until recently, primary regulatory responsibility over the export of encryption products was vested in the Department of State, which administers the International Traffic in Arms Regulations (ITAR), 22 C.F.R. 120-130.[1] In November 1996, President Clinton issued an Executive Order and Presidential memorandum transferring regulatory authority over the export of most encryption products from the Department of State to the Department of Commerce, which is responsible for administering the Export Administration Regulations (EAR), 15 C.F.R. 730-774 (1997). See Executive Order 13206, 61 Fed. Reg. 58767 (Nov. 19, 1996); 32 Weekly

[1] The ITAR controls the export of "defense articles" and "defense services." See generally Karn v. U.S. Department of State, 925 F. Supp. 1 (D.D.C. 1996), remanded, 107 F.3d 923 (D.C. Cir. 1997) (discussing application of ITAR to encryption products).

Comp. Pres. Doc. 2397 (Nov. 15, 1996) (memorandum).[2] This litigation involves the encryption export provisions that have been added to the EAR at the President's direction. We briefly summarize the general structure of the EAR, then turn to the provisions at issue in this case.[3]

a. The EAR controls the export of "dual use" items — items that can be used both for military and for civilian purposes. See 15 C.F.R. 730.3. Broadly speaking, and with various exceptions, the EAR prohibits the export of dual use items without a license from the Department of Commerce's Bureau of Export Administration (BXA). See id. § 736.2(b)(1). The EAR also controls certain other related activities involving dual use items. See id. §§ 736.2(b)(2)-(10).

For present purposes, the heart of the EAR is the Commerce Control List. See 15 C.F.R. 774 Supplement No. 1. The Commerce Control List establishes ten general

[2] The EAR is designed primarily, but not exclusively, to implement the Export Administration Act of 1979, 50 U.S.C. App. 2401 et seq. (EAA). The EAA is not permanent legislation, and when it has lapsed, the President has issued Executive Orders under the International Emergency Economic Powers Act, 50 U.S.C. 1701-1706 (IEEPA), directing and authorizing the continuation in force of the EAR. See 15 C.F.R. 730.2. Such Executive Orders are currently in effect. See Executive Order 12924, 59 Fed. Reg. 43437 (Aug. 23, 1994); 61 Fed. Reg. 68576 (Dec. 30, 1996); 62 Fed. Reg. 43629 (Aug. 13, 1997). The statutory basis for the EAR provisions at issue in this case is addressed by the district court in its opinion. See ER 552-63.

[3] Relevant provisions of the EAR are reproduced in the addendum to this brief.

categories of controlled items, such as nuclear materials (Category 1), computers (Category 4), and lasers and sensors (Category 6). Within each category, the Commerce Control List designates specific kinds of controlled items, each of which is assigned an Export Control Classification Number (ECCN). See 15 C.F.R. 738.2(d). Among other things, an item's ECCN identifies the particular reasons, such as national security or crime control, why the government controls the export of the item. See id. § 738.2(d)(2)(i).

The items on the Commerce Control List include "commodities," "software," and "technology." A "commodity" is any item other than software or technology. See 15 C.F.R. 772 (definition of "commodity"). "Software" is defined in its conventional sense. See ibid. (definitions of "software" and "program"). "Technology" is defined as "[s]pecific information necessary for the 'development,' 'production,' or 'use' of a product," including technical data and technical assistance. Ibid.

Software and technology generally are not subject to the EAR, even if they are listed on the Commerce Control List, as long as they are publicly available. See 15 C.F.R. 732.2(b), 734.3(b)(3), 734.7-734.10; see also id. Part 772 (definition of "publicly available technology and software"). The EAR also excludes from its scope printed newspapers, books, periodicals, and motion pictures. See id. § 734(b)(2). In addition, most items on the Commerce Control List that are controlled for national security reasons are eligible for national security "decontrol" if comparable items are shown to be available in sufficient quantities from foreign sources abroad. See id. Part 768.[4]

b. In December 1996, acting at the President's direction, the Department of Commerce amended the EAR to assume regulatory jurisdiction over the encryption items transferred from the jurisdiction of the Department of State. See 61 Fed. Reg. 68572 (Dec. 30, 1996). As amended, the Commerce Control List now covers encryption commodities (i.e., circuitry and other hardware) (ECCN 5A002), encryption software (ECCN 5D002), and encryption technology (ECCN 5E002).

The basic policies governing the export of encryption items under the EAR are set forth in the President's Executive Order and memorandum. The President 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. The President therefore directed that applications for licenses to export

[4] National security decontrol does not necessarily mean that an item can be exported without a license, only that it is exempt from the licensing requirements that are imposed for national security reasons.

encryption products be reviewed on a case-by-case basis by the Department of Commerce, in conjunction with other agencies, "to ensure that export * * * would be consistent with U.S. foreign policy and national security interests." Id. at 2398; see 15 C.F.R. 742.15.[5]

The President determined that "the export of encryption software, like the export of other encryption products * * * , must be controlled because of such software's functional capacity" to encrypt data, "rather than because of any possible informational value of such software * * * ." 61 Fed. Reg. 58768. The President determined that these considerations apply not only to object code but also to source code, since "encryption source code can easily and mechanically be transformed into object code." Ibid.; see p. 7 supra. The President therefore directed that all encryption software, whether in the form of source code or object code, be subject to the same export controls as encryption hardware. Ibid.; 32 Weekly Comp. Pres. Doc. at 2398.

In accordance with the President's directive, the EAR's export controls treat encryption software like encryption hardware. See generally 15 C.F.R. 742.15. This means that encryption software, unlike other kinds of software on the Commerce

[5] Certain encryption items are subject to less restrictive licensing rules and policies. See 15 C.F.R. 742.15(b)(1)-(3).

Control List, is subject to export controls even when it is publicly available in this country. See id. § 732.2(b), 734.3(b)(3); see also id. §§ 740.9(c)(3), 740.13(d)(2).[6] Encryption technology, in contrast, is exempt from export controls if it is publicly available, just as other kinds of technology are (see p. 10-11supra).

As noted above, items whose export is controlled for national security reasons are generally eligible for national security "decontrol" if comparable items are available abroad. However, the President specifically determined that "the export of encryption products * * * could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States * * * ." 61 Fed. Reg. 58767. 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 EAR's

[6] The export of encryption software consists of: (1) transferring or transmitting the software out of the United States; or (2) transferring the software to an embassy or affiliate of a foreign country. 15 C.F.R. 734.2(b)(9)(i)(A)-(B). Making encryption software available for transfer outside the United States by posting the software on the Internet constitutes an export unless adequate precautions are taken to prevent unauthorized transfer abroad. Id. § 734.2(b)(9)(ii).

foreign availability provisions "shall not be applicable with respect to export controls on such encryption products." Ibid.; see 15 C.F.R. 768.1(b). However, the Department of Commerce retains discretion to consider foreign availability of encryption products on a case-by-case basis. 61 Fed. Reg. 58767.

B. The Present Litigation

1. This case involves a challenge to the constitutionality of the EAR's controls on the export of encryption software. The plaintiff, Daniel Bernstein, is a computer science professor. As a graduate student, Bernstein created a software program, which he calls "Snuffle," that is designed to encrypt and decrypt messages interactively. Bernstein approached the Department of State to inquire about the export status of Snuffle and related explanatory materials under the ITAR (see p. 8 supra). After a series of administrative exchanges, Bernstein ultimately was informed that the source code for Snuffle could not be exported without a license, but that a license was not 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).[7]

Bernstein did not apply for an export license for his encryption program. Instead, he filed suit in the District Court for the Northern District of California in 1995 to challenge the constitutionality of the ITAR's controls on the export of encryption software and related encryption controls.

For present purposes, the most noteworthy of Bernstein's constitutional claims was a claim that the ITAR's controls on the export of encryption software amount to an unconstitutional prior restraint on speech. The "speech" at the center of this prior restraint claim is not the messages scrambled by encryption software, but rather encryption software itself — in particular, encryption source code. Bernstein contended that encryption source code is "speech" on the subject of cryptography; that the licensing requirements for the export of encryption software constitute a prior restraint on that speech; and that the prior restraint doctrine either renders the

[7] 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; see also United States v. Edler Industries, 579 F.2d 516 (9th Cir. 1978).

licensing scheme unconstitutional altogether or, alternatively, imposes a variety of strict procedural requirements on the scheme.

2. The district court issued two substantive decisions regarding Bernstein's First Amendment claims prior to the President's transfer of regulatory jurisdiction from the Department of State to the Department of Commerce. In Bernstein I, supra, the district court denied the government's motion to dismiss Bernstein's complaint. The court agreed with Bernstein that encryption source code is "speech" for First Amendment purposes. 922 F. Supp. at 1434-36. The 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 requiring a license for the export of encryption software to the prior restraints at issue in the Pentagon Papers case, New York Times v. United States, 403 U.S. 713 (1970) (per curiam), and Near v. Minnesota, 283 U.S. 697 (1931). See id. at 1438.

In Bernstein II, supra, the district court granted partial summary judgment in favor of Bernstein. In relevant part, the district court held that the ITAR's 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 licensing requirements are content-neutral regulations. Id. at 1289. However, the court held that the ITAR's licensing requirements were nonetheless facially invalid under the prior restraint doctrine because they lacked procedural safeguards that the Supreme Court has required for the licensing of parades, marches, and similar expressive activities. Id. at 1289-90.

3. Shortly after the district court issued its decision in Bernstein II, the transfer of regulatory jurisdiction to the Department of Commerce took effect. Bernstein then filed a supplemental complaint, adding the Department of Commerce as a defendant and advancing the same constitutional objections, as well as new statutory objections, to the new encryption provisions of the EAR. Bernstein did not apply to the Department of Commerce for a license to export his encryption software.

On August 25, 1997, the district court issued an opinion and order resolving Bernstein's claims concerning the EAR. ER 544-78. The court rejected Bernstein's statutory claims, holding that the EAR's controls on the export of encryption software are within the statutory authority of the President and the Department of Commerce. Id. at 552-63. However, the court held that the EAR's controls on the export of encryption source code are a facially invalid prior restraint, essentially for the same reasons that the court had invalidated the Department of State's corresponding controls in Bernstein II. Id. at 563-71.

In addition to challenging the EAR's controls on the export of encryption source code, Bernstein sought to challenge the EAR's controls on the export of encryption technology (see pp. 10-11, 13 supra). The government argued that the technology controls do not restrict any of Bernstein's activities and that Bernstein therefore lacked standing to challenge them. The district court declined to address the government's standing argument and likewise declined to address Bernstein's underlying First Amendment claims relating to the encryption technology controls. The court reasoned that the encryption technology controls are "dependent on the [EAR's] definitions and regulation of encryption commodities and software" and therefore are "unenforceable," regardless of their constitutionality, in light of the court's underlying First Amendment ruling regarding encryption source code. ER 571.

Based on its prior restraint holding, the district court issued a declaratory judgment that all provisions of the EAR that "apply to or require licensing for encryption and decryption software and related devices and technology" are unconstitutional "on the grounds of prior restraint" and "shall not be applied to

[Bernstein's] publishing of such items, including scientific papers, algorithms or computer programs * * * ." ER 574. The court enjoined the Department of Commerce from enforcing or applying the invalidated 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 * * * ." Id. at 574-75. The district court's injunction has been stayed by this Court pending appeal.

SUMMARY OF ARGUMENT

1. Encryption products, like other "dual use" products, are subject to export controls under the EAR because their use by hostile foreign governments and individuals abroad could jeopardize the national security and foreign policy interests of the United States. The EAR imposes export controls on encryption source code for the same national security and foreign policy reasons that it controls the export of other encryption products. Like other encryption products, encryption source code can be used abroad to make a computer encrypt communications and other electronic data, thereby impairing this country's foreign intelligence-gatheringcapabilities. The uncontrolled export of encryption source code is therefore inimical to fundamental national security and foreign policy interests.

The government's controls on the export of encryption source code are not an attempt to prevent the free exchange of information and ideas about cryptography. While the EAR requires a license for the export of encryption products, it does not require a license for the public dissemination or export of cryptographic information. As a result, information and ideas about cryptography are freely circulated domestically and distributed abroad: books and articles about cryptography are published, classes and lectures about cryptography are taught, and publicly available cryptographic information is sent overseas, all without the need for a license under the EAR.

Because the EAR's controls on the export of encryption source code are not aimed at the claimed capacity of source code to embody information and ideas about cryptography, but rather at the non-communicative capacity of source code to control the operation of a computer, the export controls are "content neutral" for First Amendment purposes. Content-neutral regulations are constitutional as long as they serve substantial interests that are unrelated to the suppression of speech and they do not incidentally burden substantially more speech than necessary. The EAR's export controls readily pass muster under these constitutional standards. The export controls serve fundamental national security and foreign policy interests that have nothing to do with the suppression of speech, and they are tailored to control the export of products that jeopardize those interests while leaving open ample alternative avenues for persons to communicate cryptographic information and ideas.

Instead of analyzing the EAR's export controls under the standards that govern content-neutral government regulations, the district court invoked the rubric of the prior restraint doctrine, holding that the export controls on encryption source code are facially unconstitutional on prior restraint grounds. That holding is fundamentally misconceived. Unlike the classic prior restraints at issue in cases like New York Times v. United States, 403 U.S. 713 (1970), which were intended to prevent speakers from conveying disfavored information and ideas to the public, the EAR's export controls are not an attempt to prevent the free exchange of information and ideas about cryptography. And unlike the licensing schemes at issue in cases like City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750 (1988), the EAR's export controls do not single out expression and expressive activities for unique regulatory burdens. Because the EAR is a law of general application that does not target expression, the decisions of the Supreme Court and this Court make clear that it is not subject to facial invalidation on prior restraint grounds.

2. Even if the district court's underlying First Amendment holding were correct, the declaratory and injunctive relief granted by the district court would be invalid, because it far exceeds the scope of the court's own First Amendment reasoning. The district court's reasoning applies only to encryption source code, but read literally, the declaratory judgment and injunction cover the EAR's controls on all encryption items. Because the district court's reasoning does not apply to items other than source code, the declaratory judgment and injunction would have to be narrowed accordingly even if the district court's First Amendment holding were accepted.

ARGUMENT[8]

I. THE EAR'S CONTROLS ON THE EXPORT OF ENCRYPTION SOURCE CODE DO NOT VIOLATE THE FIRST AMENDMENT

This Court has warned that "'[t]he phrase "prior restraint" is not a self-wielding sword[,] [n]or can it serve as a talismanic test.'" Information Providers' Coalition v. FCC, 928 F.2d 866, 877 (9th Cir. 1991) (quoting Kingsley Books, Inc. v. Brown, 354 U.S. 436, 441 (1957)). This case illustrates the wisdom of that warning. The EAR's encryption export controls are designed not to prevent the public exchange of information and ideas about cryptography, but rather to control the export of products that can be used abroad to encrypt data and thereby compromise this country's national security and foreign policy interests. As we show below, the export controls at issue are content-neutral regulations whose effect on expressive activities, if any,

[8] The constitutional issues addressed in this brief regarding the EAR's encryption export controls were raised, inter alia, in the parties' cross-motions for summary judgment and were ruled on by the district court in its opinion and order of August 25, 1997. The constitutionality of federal regulations is subject to de novo review by this Court. See, e.g., International Brotherhood of Teamsters v. Department of Transportation, 932 F.2d 1292, 1298 (9th Cir. 1991). The grant of a permanent injunction is subject to reversal if, inter alia, it rests on erroneous legal conclusions. See, e.g., Multnomah Legal Services Workers Union v. Legal Services Corp., 936 F.2d 1547, 1552 (9th Cir. 1991); Sports Form, Inc. v. United Press International, Inc., 686 F.2d 750, 752 (9th Cir. 1982) ("all conclusions of law [underlying a permanent injunction] are freely reviewable").

is merely incidental and entirely permissible. The controls on the export of encryption products, including encryption source code, have nothing to do with censoring speech and do not present the risks that underlie the prior restraint doctrine. The district court's prior restraint ruling therefore is not simply "novel," as the district court itself acknowledged, but fundamentally mistaken.[9]

A. The EAR's Export Controls Are Constitutionally Permissible Content-Neutral Regulations

1. The First Amendment draws a sharp distinction between content-based and content-neutral laws. When the government seeks to "suppress, disadvantage, or impose differential burdens on speech because of its content," the First Amendment ordinarily subjects such efforts to strict scrutiny. Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 642 (1994). "In contrast, regulations that are unrelated to the content of speech" are subject to less demanding First Amendment scrutiny, because

[9] Given the foreign locus of the EAR's export controls and the national security concerns that underlie them, it is not clear that the First Amendment applies with full force in this case. See Haig v. Agee, 453 U.S. 280, 308 (1981) (declining to decide whether "First Amendment protections reach beyond our national boundaries"); see also Bullfrog Films, Inc. v. Wick, 847 F.2d 502, 509 n.9 (9th Cir. 1988) (approving district court holding that First Amendment applies with equal force to speech directed abroad "in the absence of some overriding governmental interest such as national security") (emphasis added). However, this Court need not resolve that issue, for as we show below, the EAR's export controls are constitutional even if it is assumed that the First Amendment applies with full force.

they ordinarily "pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue." Ibid.

A regulation is content-neutral "if it is 'justified without reference to the content of the regulated speech.'" One World One Family Now v. City and County of Honolulu, 76 F.3d 1009, 1012 (9th Cir.), cert. denied, 117 S. Ct. 554 (1996) (quoting Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984)); Kev, Inc. v. Kitsap County, 793 F.2d 1053, 1058-59 (9th Cir. 1986). The government's purpose in imposing the restriction "is the controlling consideration" in this inquiry. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989). "The test is whether the government has adopted the restriction 'because of disagreement with the message [the speech] conveys.'" One World, 76 F.3d at 1012 (quoting Ward, 491 U.S. at 791). A law "'that serves purposes unrelated to the content of expression is deemed neutral[] even if it has an incidental effect on some speakers or messages but not others.'" Ibid.

When measured against these benchmarks, the EAR's controls on the export of encryption products, including encryption source code, manifestly are content neutral. As noted above, the President has determined that the use of encryption products 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 government's object in controlling the export of encryption products is not to prevent the free exchange of information and ideas about cryptography, but rather to minimize the risk that our national security and foreign policy interests will be compromised by the use abroad of encryption products produced in this country.

Encryption software, including encryption source code, is subject to export controls for the same reasons as encryption hardware. The President has directed the Department of Commerce to control the export of encryption software "because of such software's functional capacity" to enable computers to encrypt data, a capacity that it shares with encryption hardware, "rather than because of any possible informational value of such software." Executive Order 13206, 61 Fed. Reg. 58768 (Nov. 19, 1996). Because encryption source code "can easily and mechanically be transformed into object code," it has the same capacity to make computers encrypt data, and it is subject to export controls for that reason. Ibid.[10]

[10] The district court itself recognized "the ease with which one can convert source code into object code." Bernstein I, 922 F. Supp. at 1434 n.14.

It is true, as noted above, that source code (unlike object code) can be read and understood by persons, such as computer scientists and programmers, who are trained in the particular programming language in which the source code is written. However, source code remains a sequence of instructions to a computer, and it is routinely written, distributed, and used for the wholly non-expressive purpose of making a computer carry out specified tasks — here, the task of encrypting data. As the parties stipulated below, "[c]ryptographic 'source code' is a computer program written in a computer language * * * that can be used to encrypt and decrypt information." ER 301 (emphasis added). Moreover, recipients of encryption source code do not have to be able to read and understand it in order to use it to encrypt data. Because source code can be converted into object code by the computer itself (see p. 7 supra), a person who is given encryption source code on a floppy disk or other electronic medium can load the source code into his computer, convert it into object code, and execute the program without reading the source code or understanding the sequence of computer instructions that it contains.[11]

[11] By distributing a software program in the form of source code, a programmer can make the program available for use on a potentially wide range of computer hardware. In contrast, once a program has been converted into object code, it typically (although not invariably) can be run only on a particular kind of computer (or, more precisely, a particular kind of microprocessor). Distributing a program in

Source code is therefore fundamentally different from blueprints, recipes, and other "how-to" materials. A blueprint cannot be used to make a building unless a person reads and understands it; it cannot do anything other than convey information to human beings. Similarly, a recipe cannot be used to make a casserole or a cake unless it is read by a person who understands the information it contains and who acts on the basis of that information. Source code, in contrast, can be used to control the operation of a computer without conveying information to the user. When the district court equated source code with "instructions, do-it-yourself manuals, [and] recipes" (Bernstein I, 922 F. Supp. at 1435), it failed to grasp this basic distinction.

The EAR's controls on the export of encryption source code thus do not depend, even indirectly, on the information or ideas that may be claimed to be embodied in the source code. Simply stated, the EAR controls the export of encryption source code because of what it does, not because of what (if anything) it says.

The design and operation of the EAR's encryption provisions confirm that the EAR does not control the export of encryption source code "because of disagreement

the form of source code therefore can increase the program's practical utility to users by making it more "portable."

with the message it conveys." Ward, 491 U.S. at 791. The EAR treats encryption source code exactly like encryption object code and encryption hardware, which are not even arguably used as a means of expressing and conveying ideas about cryptography. See 15 C.F.R. 742.15; see also pp. 45-47 infra. At the same time, the EAR does not attempt to restrict the free flow of public information and ideas about cryptography, either domestically or internationally. Information that can be used in the design and operation of encryption products — in the parlance of the EAR, encryption "technology" — is not subject to the EAR's controls, and therefore may be freely exported, as long as it is publicly available. See 15 C.F.R. 734.3(b)(3). Technology is "publicly available" if, inter alia, it is published or otherwise is generally accessible to the interested public in any form (id. § 734.7(a)); it is a product of fundamental research (id. § 734.8); or it is distributed through academic instruction (id. § 734.9). See pp. 10-11 supra. In addition, the EAR excludes books, magazines, and other printed materials on all subjects, thereby giving carte blanche to the export of publications on cryptography. See id. § 734.3(b)(2). In short, the EAR goes out of its way to distinguish between the export of encryption products, which requires a license, and the public dissemination of cryptographic information, which does not. This regulatory scheme obviously is not the product of government hostility toward the subject of cryptography or the free exchange of ideas on that subject.

2. A content-neutral government regulation 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 restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.'" Turner, 512 U.S. at 662 (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)). "To satisfy this standard, a regulation need not be the least speech-restrictive means of advancing the Government's interests. 'Rather, the requirement of narrow tailoring is satisfied "so long as the * * * regulation promotes a substantial government interest that would be achieved less effectively absent the regulation."'" Ibid. (quoting Ward, 491 U.S. at 799). A regulation is narrowly tailored as long as "the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" Ibid.

The district court originally suggested, without deciding, that these "relatively mild" standards do not apply here because encryption source code "is speech and not conduct." Bernstein I, 922 F. Supp. at 1437. As the foregoing discussion indicates, characterizing source code as "speech" rather than "conduct" is far too simplistic: source code consists of instructions to a computer, it can be used to make a computer perform tasks without conveying information to human beings, and it can be exported for entirely non-expressive purposes. In any event, the appropriate level of First Amendment scrutiny depends not on whether the government is regulating "speech" or "conduct," but instead on the purpose of the government regulation. See, e.g., Blount v. SEC, 61 F.3d 938, 942 (D.C. Cir. 1995), cert. denied, 116 S. Ct. 1351 (1996) ("This [purpose-based] methodology has come to replace the distinction between speech [regulations] and conduct regulations"); Home Box Office, Inc. v. FCC, 567 F.2d 9, 47-48 (D.C. Cir.) (per curiam), cert. denied, 434 U.S. 829 (1977); see also John Hart Ely, Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis, 88 Harv. L. Rev. 1482, 1496-97 (1975). As long as the regulation is not animated by a desire to suppress disfavored messages, it is subject to intermediate rather than strict scrutiny even if it unquestionably regulates speech. See, e.g., Turner, 512 U.S. at 641-61 (applying intermediate scrutiny to regulations requiring cable operators to carry broadcast television programming); Ward, 491 U.S. at 790-803 (applying intermediate scrutiny to regulations restricting volume of music played in outdoors concerts).

The EAR's controls on the export of encryption software, including encryption source code, readily pass constitutional muster under the First Amendment standards governing content-neutral regulations. First, they plainly "'further[] an important or substantial governmental interest'" (Turner, 512 U.S. at 662). "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." Haig v. Agee, 453 U.S. 280, 307 (1981). Here, the government has a compelling interest in controlling the export of encryption products to hostile countries, organizations, and individuals whose use of such products abroad could jeopardize our national security and foreign policy.[12] As the Deputy Director of the NSA has explained, the use of encryption products by foreign intelligence targets "can have a debilitating effect on NSA's ability to collect and report * * * critical foreign intelligence." ER 96. Absent the kind of licensing requirements contained in the EAR, domestic producers of encryption software could engage in the unrestricted export of their products to any person abroad for any reason, regardless

[12] As a constitutional matter, the authority to restrict exports for reasons of national security and foreign policy finds its origins both in Article I and in Article II. See Art. I, § 8, cl. 3, 11-14; Art. II, § 2, cl. 1.

of a particular encryption product's strength and its potential attractiveness to hostile interests abroad.[13]

The value of controlling the export of encryption software and other encryption products is not negated by the mere fact that some encryption products are also available from foreign sources abroad. As noted above, the President has expressly determined that the uncontrolled 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, 61 Fed. Reg. 58767 (Nov. 19, 1996). The existing availability of particular encryption products abroad says nothing about how widely such products are used or how effective such products may be.[14] Nor does it imply that this country's intelligence-

[13] Even if the person exporting the software does not intend or expect that the software will be used for purposes contrary to this country's national security and foreign policy interests, he has no direct control over the use to which the software will be put once it has been exported, particularly if the software is made available for unrestricted downloading via the Internet.

[14] As noted above, the President has determined that "facts and questions concerning the foreign availability of [comparable] 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." Executive Order 13206, 61 Fed. Reg. 58767 (Nov. 19, 1996). A full inquiry into the "comparability" of particular foreign encryption products could not be undertaken without revealing details about the NSA's existing cryptanalysis

gathering capabilities would be unimpaired by the uncontrolled export of all encryption software products, regardless of their strength and usefulness abroad. Even if foreign availability were assumed to be relevant to the grant of denial of an export license in an individual case, it is irrelevant to whether exports should be subject to a licensing requirement in the first instance.[15]

In addition to being substantial, the interests served by the EAR's export controls are obviously "unrelated to the suppression of free expression'" (Turner, 512 U.S. at 662). As shown above, the EAR controls the export of encryption software, including encryption source code, because of its capacity to make computers encrypt data, not because of any information or ideas about cryptography that it may be claimed to embody or convey. The EAR's controls are not designed to (and do not) suppress the free exchange of ideas about cryptography, either among computer scientists or among members of the public. See ER 108-297, 305-419 (examples of books, articles, and academic courses on cryptography).

capabilities — extraordinarily sensitive information that is, for obvious reasons, subject to the most stringent security measures.

[15] As noted above, while encryption products are not covered by the EAR's general foreign-availability decontrol procedures, the President has given the Department of Commerce the discretion to consider the significance of foreign availability on a case-by-case basis (see p. 14 supra).

Finally, the EAR's export controls are narrowly tailored. As noted above, the narrow tailoring requirement is satisfied if the government's interests ""would be achieved less effectively absent the regulation."" Turner, 512 U.S. at 662 (quoting Ward, 491 U.S. at 799). That is obviously the case here. As explained above, encryption software on a computer diskette or similar electronic media can be converted from source code into object code at the press of a button, thereby enabling computers to scramble messages and other data (see pp. 7-8 supra). Elimination of export controls on encryption source code would permit the unrestricted export of encryption software to any person, organization, or country, without regard to the strength of the software, the identity of the recipients, or the uses to which they could be expected to put it. The detrimental impact on the national security and foreign policy interests identified by the President (see p. 12 supra) requires no elaboration.

The EAR's export controls "do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" Turner, 512 U.S. at 662 (quoting Ward, 491 U.S. at 799). The export controls are targeted at precisely the activity that threatens the government's legitimate interests — the export of products that have the capability of shielding foreign intelligence targets from American intelligence-gathering efforts. The EAR does not prohibit the export of encryption products altogether, but rather establishes a licensing system under which exports that are consistent with our national security and foreign policy interests may go forward. See 15 C.F.R. 742.15(b) (encryption export license applications reviewed "to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests"). The licensing requirements are tailored to the risks presented, with less restrictive requirements for exports that pose lesser risks. See id. § 742.15(b)(1)-(3). Finally, the EAR's provisions regarding encryption technology "leave open ample alternative channels of communication" (Ward, 491 U.S. at 802) for the exchange of information and ideas regarding cryptography (see pp. 29-30 supra; see also pp. 49-50 infra). The EAR's export controls are therefore sufficiently tailored to satisfy intermediate First Amendment scrutiny.

B. The EAR's Export Controls Are Not A Facially Unconstitutional Prior Restraint

The district court did not dispute that the EAR's controls on the export of encryption software, including encryption source code, are content-neutral regulations that are not aimed at the suppression of speech. ER 569; Bernstein II, 945 F. Supp. at 1288-89. The court nevertheless held that the controls must be struck down as an unconstitutional prior restraint. In so holding, the district court did not find that the government had used its licensing authority to deter the expression of disfavored ideas about cryptography, either by Bernstein or by anyone else. Instead, the court held that the export controls are unconstitutional on their face, without regard to how they have been or may be applied in any particular case. That holding is fundamentally misconceived.

1. The district court originally sought to analogize controls on the export of encryption source code to the classic prior restraints presented in cases such as New York Times v. United States, 403 U.S. 713 (1970) (per curiam), and Near v. Minnesota, 283 U.S. 697 (1931). See Bernstein I, 922 F. Supp. at 1438. However, the EAR's export controls are fundamentally different, both in purpose and in effect, from the prior restraints at issue in such cases.

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 traditional prior restraint cases, the government's underlying object was to prevent speakers from communicating disfavored information and ideas to the public. These 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 chiefly 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 controls on the export of encryption source code and other encryption products are manifestly not aimed at preventing the free exchange of information and ideas about cryptography. As explained above, the EAR is concerned with controlling the export of products that encrypt data, not with obstructing the public dissemination of cryptographic knowledge. The exclusion of publicly available technology and printed materials from the scope of the EAR (see pp. 10-11 supra) ensures that licensing requirements for the export of encryption products cannot be used to keep cryptographic information out of the hands of computer scientists or the public at large, either here or abroad. This scheme simply bears no meaningful resemblance to the efforts to restrain speech in cases like New York Times and Near.

2. In addition to relying on traditional prior restraint cases, the district court also looked to cases involving licensing requirements for expressive activities like leafleting, parades, and marches. See ER 565, 569-70. However, none of these cases supports the district court's facial invalidation of the EAR's controls on the export of encryption software. The cases on which the district court relied do not hold that every licensing scheme is subject to a facial challenge, rather than an as-applied challenge, on prior restraint grounds. To the contrary, they make clear that facial challenges are permissible only when a licensing scheme is directed narrowly and specifically at expressive activities — something that the EAR's encryption export controls simply do not do.

The Supreme Court's decision in City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750 (1988) establishes the standards for "distinguish[ing] laws that are vulnerable to facial challenge [on prior restraint grounds] 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, but rather may be challenged only on an as-applied basis. Id. at 760-61. Thus, for example, a law requiring building permits is not subject to facial challenge on prior restraint grounds, even though it restrains activities that may be associated with speech (such as the construction of a newspaper printing plant or a movie theater) and even though it could be used in an unusual case for the purpose of restraining speech or expressive activities. Id. at 762. In sum, under Lakewood, "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.'" Roulette v. City of Seattle, 97 F.3d 300, 305 (9th Cir. 1996) (emphasis added) (quoting Lakewood, 486 U.S. at 760).

Applying these standards, the EAR's export controls are not subject to facial invalidation under the prior restraint doctrine. To begin with, the specific activity underlying the district court's ruling — the export of encryption source code— cannot fairly be said to be activity "commonly associated with expression." As explained above, source code is a set of instructions to a computer, and it is commonly written and distributed for the wholly non-expressive purpose of controlling a computer's operation. We do not mean to suggest that the export of encryption source code may never be undertaken for expressive purposes. But it nonetheless stands in obvious contrast to activities such as parading, posting signs, or distributing handbills, which are always (or almost always) undertaken for expressive purposes.

Moreover, even if it were assumed for the sake of argument that the export of encryption source code is ordinarily an expressive activity, the EAR's export controls are not "directed narrowly and specifically" (Lakewood, 486 U.S. at 760) at that activity. The EAR's controls on the export of encryption source code are simply part and parcel of its general controls on the export of encryption products. Instead of singling out encryption source code from other encryption items, the EAR expressly provides that the export of encryption software (source code and object code) is to be controlled just like the export of encryption hardware. 15 C.F.R. 742.15. In turn, encryption products form only a tiny part of the vast range of "dual use" items whose export is controlled by the EAR. See generally 15 C.F.R. Part 774, Supplement No. 1 (Commerce Control List).[16]

[16] For example, the EAR covers such diverse 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).

Far from singling out expressive activities, the EAR is thus a perfect example of a "law[] of general application * * * not aimed at conduct commonly associated with expression" (Lakewood, 486 U.S. at 760-61). The district court's insistence that "[t]he encryption regulations * * * [are] specifically directed at speech protected by the First Amendment" (ER 567) simply disregards the breadth and generality of the regulatory scheme. The most that may be said is that this general licensing scheme includes within its broad scope a particular activity (the export of encryption source code) that could be, but need not be and often is not, undertaken for expressive purposes. It does not follow that the licensing scheme is therefore subject to facial invalidation on prior restraint grounds, any more than a building permit scheme 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 761.

The EAR stands in direct contrast to the kinds of licensing schemes that have been subjected to facial invalidation by the Supreme Court and this Court. The Supreme Court has entertained facial challenges to laws requiring licenses for the distribution of handbills and newspapers; laws requiring licenses for public speeches and parades; and laws licensing businesses engaged in sexually explicit speech. See, e.g., Lakewood (licensing distribution of newspapers on public property); FW/PBS, Inc. v. City of Dallas, 493 U.S. 215 (1990) (licensing scheme that "largely targets businesses purveying sexually explicit speech"); Forsyth County v. Nationalist Movement, 505 U.S. 123 (1992) (licensing public speeches and parades); Shuttlesworth v. City of Birmingham, 394 U.S. 147 (1969) (licensing parades); Lovell v. Griffin, 303 U.S. 444 (1938) (licensing distribution of literature). This Court has entertained facial challenges to similar licensing schemes.[17] In each of these cases, the laws in question have been directed at expression or conduct commonly associated with expression, and the laws have either confined their scope to expressive activities or have singled them out for special burdens. The EAR does nothing of the kind.

[17] See Desert Outdoor Advertising, Inc. v. City of Moreno Valley, 103 F.3d 814, 816-17 (9th Cir. 1996), cert. denied, 65 U.S.L.W. 3666 (Oct. 14, 1997) (posting commercial signs); Grossman v. City of Portland, 33 F.3d 1200, 1201 (9th Cir. 1994) (speaking and demonstrating in public park); Gerritson v. City of Los Angeles, 994 F.2d 570, 573-74 (9th Cir.), cert. denied, 510 U.S. 915 (1993) (distributing handbills); Gaudiya Vaishnava Society v. City and County of San Francisco, 952 F.2d 1059, 1062 (9th Cir. 1990), cert. denied, 504 U.S. 914 (1992) ("charitable sales solicitation"); Carreras v. City of Anaheim, 768 F.2d 1039, 1041-42, 1047-50 (9th Cir. 1985) (soliciting charitable donations); Rosen v. Port of Portland, 641 F.2d 1243, 1244-45 & n.2 (9th Cir. 1981) (soliciting donations and speaking in airports).

The district court noted that the EAR treats encryption software differently from, and in certain respects more restrictively than, other kinds of software listed on the Commerce Control List. ER 567; see pp. 6-7 supra. But this differential treatment does not justify the facial invalidation of the EAR's encryption software provisions. As explained above, the EAR 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 refraining from regulating it on the basis of its potential informational value is to turn the logic of the prior restraint doctrine on its head.

II. THE DISTRICT COURT'S DECLARATORY AND INJUNCTIVE RELIEF IS TOO BROAD

For the foregoing reasons, the district court erred in concluding that the EAR's controls on the export of encryption source code are facially unconstitutional under the First Amendment. The judgment of the district court therefore should be reversed. Even if the district court's First Amendment ruling were correct, however, the court's declaratory judgment and injunction would nonetheless require modification, for the relief granted by the district court is unduly broad even if the court's First Amendment reasoning is accepted.

A. Encryption Object Code and Encryption Commodities

1. Read literally, the declaratory judgment and injunction apply to the EAR's controls on the export of encryption "software," a term that the EAR uses to encompass not only source code but also object code. ER 574 ("encryption and decryption software"); see 15 C.F.R. 772 (definition of "encryption software"). Even when taken on its own terms, however, the district court's prior restraint theory has no applicability to object code. Unlike source code, object code is a sequence of binary digits (0s and 1s) that effectively can be "read" only by computer microprocessors. See, e.g., Sega Enterprises, 977 F.2d at 1525 ("humans cannot read object code") (emphasis in original); ISC-Bunker Ramo Corp. v. Altech, Inc., 765 F. Supp. 1310, 1316 (N.D. Ill. 1990) (object code "is virtually unintelligible to people"). Object code is not used by computer scientists or anyone else to represent and convey information and ideas about programming and computer science. The export of object code therefore simply cannot be regarded as "speech," even under the district court's First Amendment theory.[18]

It is possible that the district court meant to refer only to source code and was merely speaking imprecisely when it used the broader term "software." But whether the court's use of "software" was inadvertent or intentional, it was erroneous in either case. The declaratory judgment and injunction therefore must be modified to exclude controls on the export of encryption object code.

2. The declaratory judgment and injunction also cover the EAR's controls on the export of "related devices." See ER 574 ("encryption and decryption software and related devices"). "Device" is not a defined term under the EAR, and it is not entirely clear what the district court had in mind when it used the term. However, it is possible that the court meant to refer to encryption "commodities" — that is, hardware products (such as electronic circuitry) that encrypt data. See 15 C.F.R. Part 774 Supplement No. 1, ECCN 5A002. Encryption commodities fall outside the scope

[18] In Bernstein I, the district court stated in passing that object code "operates as a 'language.'" 922 F. Supp. at 1435. But even if object code is a "language" in an abstract sense, it is a language that effectively cannot be understood by humans and is not used by them to communicate with one another. For that reason, its export simply does not constitute "speech" in any sense that is relevant to the First Amendment.

of the district court's First Amendment reasoning for the same reasons that encryption object code does: electronic circuitry and other hardware do not themselves express ideas about cryptography and are not distributed to convey such ideas. The declaratory judgment and injunction therefore must also be modified to exclude controls on the export of encryption commodities.

B. Encryption Technology

1. In addition to encryption software and "related devices," the district court's declaratory judgment and injunction also cover encryption technology. See ER 571, 574. As noted above, the district court did not address the merits of Bernstein's First Amendment challenge to the export controls on encryption technology, nor did it decide whether Bernstein had standing to pursue that challenge in the first instance. Instead, the court reasoned that its underlying First Amendment ruling regarding encryption source code rendered the export controls on encryption technology "unenforceable." Id. at 571.

That reasoning is obviously wrong. Encryption technology is "information necessary for the 'development,' 'production,' or 'use'" (15 C.F.R. 772) of any encryption product — meaning not only encryption source code, but also encryption object code and encryption commodities (hardware). As we have just shown, even under the district court's own reasoning, the EAR's controls on the export of encryption object code and encryption commodities should be unaffected. As a result, the controls on encryption technology should likewise be unaffected, since encryption technology can be used "for the 'development,' 'production,' or 'use'" of encryption object code or encryption commodities.

2. The district court's wholesale invalidation of the EAR's encryption technology controls is particularly ironic because, as the government showed below, Bernstein lacks standing to challenge the technology controls in the first place. In order to have standing under Article III, a plaintiff must establish, inter alia, that the defendant's actions have injured him. See, e.g., Bennett v. Spear, 117 S. Ct. 1154, 1161 (1997). Simply stated, the EAR's controls on encryption technology, as distinct from the controls on encryption software, do not restrict the academic activities in which Bernstein is engaged and therefore cannot be claimed to have caused him any cognizable injury.

As explained above, the EAR does not control the export of "publicly available" technology, including encryption technology. 15 C.F.R. 734.3(b)(3). Technology is considered "publicly available" if it is "released by instruction in catalog courses and associated teaching laboratories of academic institutions." Id.

§ 734.9. Technology is also "publicly available" if it is the product of "fundamental research," meaning basic and applied research whose results are "ordinarily published and shared broadly within the scientific community." Id. § 734.8(a). Finally, technology is "publicly available" when it "already [is] published or will be published" and thereby made "generally accessible to the interested public in any form * * * ." Id. §§ 734.3(b)(3)(i), 734.7(a). These provisions exclude from the scope of the EAR all of the basic avenues of academic discourse — classroom instruction, basic research, and publication.

In light of these provisions, it should come as no surprise that academic activities relating to cryptography are flourishing and are not being restricted by the government. The record below contains extensive and unrebutted evidence that cryptography is the subject of numerous college courses, academic symposia, textbooks, and fundamental research published in scholarly journals. See ER 108-297, 305-419. The record confirms that the EAR's technology controls do not limit the free public exchange of information and ideas about cryptography.

In the proceedings below, Bernstein suggested that his classroom activities are restricted by 15 C.F.R. 744.9. Under that provision, a license must be obtained to provide technical assistance to foreigners "with the intent to aid a foreign person in the development or manufacture" of controlled encryption software or commodities outside the United States. Bernstein suggested that this provision might restrict classroom instruction about cryptography when foreign students are in attendance. However, 15 C.F.R. 744.9 specifically provides that "the mere teaching or discussion of information about cryptography, including, for example, in an academic setting, by itself would not establish the [requisite] intent * * * , even where foreign persons are present." Ibid. (emphasis added). As a result, 15 C.F.R. 744.9 does not require Bernstein to obtain a license in order to disseminate information about cryptography for academic purposes in his classroom, even if foreign students are enrolled.[19]

Even if Bernstein had standing to challenge 15 C.F.R. 744.9, that challenge would be foreclosed by this Court's decision in United States v. Edler Industries, 579 F.2d 516 (9th Cir. 1978). In Edler, this Court rejected a First Amendment challenge

[19] For that matter, the EAR does not require Bernstein to obtain a license in order to distribute encryption source code for instructional purposes in his classroom or other academic settings in the United States. As noted above, the domestic distribution of encryption software does not constitute an "export" unless the software is being given to an embassy or agent of a foreign country. See 15 C.F.R. 734.2(b)(9)(i)(B). Thus, Bernstein's domestic distribution of encryption source code to foreign students and colleagues does not constitute an export unless they are acting as agents for foreign governments. The district court was therefore incorrect when it stated (ER 566) that the EAR imposes a prior restraint on the use of encryption source code in "teaching a class" or "speaking at conferences."

to export controls administered by the Department of State under the International Trade in Arms Regulations (ITAR) (see p. 8 supra). The regulations prohibited "the provision of technical assistance for the foreign manufacture of articles that, if manufactured domestically, would [themselves] be" subject to export controls under the ITAR. 579 F.2d at 521. As construed by this Court, the technical assistance prohibition applied when the party providing the technical assistance "know[s] or has reason to know that [the] information is intended [by the recipient] for the prohibited use." Id. at 521. The Court held that, so construed, the technical assistance provisions "do not interfere with constitutionally protected speech." Ibid. The Court held specifically that the controls "are not overbroad" and "are not an unconstitutional prior restraint on speech." Ibid. See also United States v. Posey, 864 F.2d 1487, 1496-97 (9th Cir. 1989) (reaffirming Edler's First Amendment holding).

The restriction on technical assistance contained in 15 C.F.R. 744.9 is indistinguishable, for First Amendment purposes, from the restriction on technical assistance sustained by this Court in Edler. Like the provision at issue in Edler, 15 C.F.R. 744.9 restricts technical assistance directed at the foreign production of products that themselves are subject to export controls. And 15 C.F.R. 744.9 contains a scienter requirement that is even more protective than the "know or have reason to know" standard approved in Edler: a license is required only when the person providing the technical assistance "with the intent" to aid in the foreign production of controlled products (emphasis added). It thus follows a fortiori from Edler that 15 C.F.R. 744.9 does not violate the First Amendment.

CONCLUSION

For the foregoing reasons, the judgment of the district court should be reversed. In the alternative, the declaratory judgment and injunction issued by the district court should be modified to exclude items other than encryption source code.

Respectfully submitted,

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

STEPHEN W. PRESTON
Deputy Assistant Attorney General

DOUGLAS N. LETTER
SCOTT R. McINTOSH
Attorneys, Appellate Staff
Civil Division, Room 9550
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530-0001

October 16, 1997

STATEMENT OF RELATED CASES

Counsel for the appellants is not aware of any related case pending in this Court.

ADDENDUM

15 C.F.R. § 734.2 Important EAR terms and principles.

(a) Subject to the EAR--Definition.

(1) "Subject to the EAR" is a term used in the EAR to describe those items and activities over which BXA exercises regulatory jurisdiction under the EAR. Conversely, items and activities that are not subject to the EAR are outside the regulatory jurisdiction of the EAR and are not affected by these regulations. The items and activities subject to the EAR are described in § 734.2 through § 734.5 of this part. You should review the Commerce Control List (CCL) and any applicable parts of the EAR to determine whether an item or activity is subject to the EAR. However, if you need help in determining whether an item or activity is subject to the EAR, see § 734.6 of this part. Publicly available technology and software not subject to the EAR are described in § 734.7 through § 734.11 and Supplement No. 1 to this part.

(2) Items and activities subject to the EAR may also be controlled under export-related programs administered by other agencies. Items and activities subject to the EAR are not necessarily exempted from the control programs of other agencies. Although BXA and other agencies that maintain controls for national security and foreign policy reasons try to minimize overlapping jurisdiction, you should be aware that in some instances you may have to comply with more than one regulatory program.

(3) The term "subject to the EAR" should not be confused with licensing or other requirements imposed in other parts of the EAR. Just because an item or activity is subject to the EAR does not mean that a license or other requirement automatically applies. A license or other requirement applies only in those cases where other parts of the EAR impose a licensing or other requirement on such items or activities.

(b) Export and reexport--

(1) Definition of export. "Export" means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States, as described in paragraph (b)(2)(ii) of this section. See part 772 of the EAR for the definition that applies to exports of satellites subject to the EAR. See paragraph (b)(9) of this section for the definition that applies to exports of encryption source code and object code software subject to the EAR.

(2) Export of technology or software. (See paragraph (b)(9) for provisions that apply to encryption source code and object code software.) "Export" of technology or software, excluding encryption software subject to "EI" controls, includes:

(i) Any release of technology or software subject to the EAR in a foreign country; or

(ii) Any release of technology or source code subject to the EAR to a foreign national. Such release is deemed to be an export to the home country or countries of the foreign national. This deemed export rule does not apply to persons lawfully admitted for permanent residence in the United States and does not apply to persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)). Note that the release of any item to any party with knowledge a violation is about to occur is prohibited by § 736.2(b)(10) of the EAR.

(3) Definition of "release" of technology or software. Technology or software is "released" for export through:

(i) Visual inspection by foreign nationals of U.S.-origin equipment and facilities;

(ii) Oral exchanges of information in the United States or abroad; or

(iii) The application to situations abroad of personal knowledge or technical experience acquired in the United States.

(4) Definition of reexport. "Reexport" means an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country; or release of technology or software subject to the EAR to a foreign national outside the United States, as described in paragraph (b)(5) of this section. See part 772 of the EAR for the definition that applies to reexports of satellites subject to the EAR.

(5) Reexport of technology or software. Any release of technology or source code subject to the EAR to a foreign national of another country is a deemed reexport to the home country or countries of the foreign national. However, this deemed reexport definition does not apply to persons lawfully admitted for permanent residence. The term "release" is defined in paragraph (b)(3) of this section. Note that the release of any item to any party with knowledge or reason to know a violation is about to occur is prohibited by § 736.2(b)(10) of the EAR.

(6) For purposes of the EAR, the export or reexport of items subject to the EAR that will transit through a country or countries or be transshipped in a country or countries to a new country or are intended for reexport to the new country, are deemed to be exports to the new country.

(7) If a territory, possession, or department of a foreign country is not listed on the Country Chart in Supplement No. 1 to part 738 of the EAR, the export or reexport of

items subject to the EAR to such destination is deemed under the EAR to be an export to the foreign country. For example, a shipment to the Cayman Islands, a dependent territory of the United Kingdom, is deemed to be a shipment to the United Kingdom.

(8) Export or reexport of items subject to the EAR does not include shipments among any of the states of the United States, the Commonwealth of Puerto Rico, or the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States. These destinations are listed in Schedules C & E, Classification of Country and Territory Designations for U.S. Export Statistics, issued by the Bureau of the Census.

(9) Export of encryption source code and object code software.

(i) For purposes of the EAR, the export of encryption source code and object code software means:

(A) An actual shipment, transfer, or transmission out of the United States (see also paragraph (b)(9)(ii) of this section); or

(B) A transfer of such software in the United States to an embassy or affiliate of a foreign country.

(ii) The export of encryption source code and object code software controlled for EI reasons under ECCN 5D002 on the Commerce Control List (see Supplement No. 1 to part 774 of the EAR) includes downloading, or fcausing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photooptical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States. Such precautions shall include:

(A) Ensuring that the facility from which the software is available controls the access to and transfers of such software through such measures as:

(1) The access control system, either through automated means or human intervention, checks the address of every system requesting or receiving a transfer and verifies that such systems are located within the United States;

(2) The access control system, provides every requesting or receiving party with notice that the transfer includes or would include cryptographic software subject to export controls under the Export Administration Act, and that anyone receiving such a transfer cannot export the software without a license; and

(3) Every party requesting or receiving a transfer of such software must acknowledge affirmatively that he or she understands that the cryptographic software is subject to export controls under the Export Administration Act and that anyone receiving the transfer cannot export the software without a license; or

(B) Taking other precautions, approved in writing by the Bureau of Export Administration, to prevent transfer of such software outside the U.S. without a license.

15 C.F.R. § 734.3 Items subject to the EAR.

(a) Except for items excluded in paragraph (b) of this section, the following items are subject to the EAR:

(1) All items in the United States, including in a U.S. Foreign Trade Zone or moving intransit through the United States from one foreign country to another;

(2) All U.S. origin items wherever located;

(3) U.S. origin parts, components, materials or other commodities incorporated abroad into foreign-made products, U.S. origin software commingled with foreign software, and U.S. origin technology commingled with foreign technology, in quantities exceeding de minimis levels as described in § 734.4 and Supplement No. 2 of this part;

(4) Certain foreign-made direct products of U.S. origin technology or software, as described in § 736.2(b)(3) of the EAR. The term "direct product" means the immediate product (including processes and services) produced directly by the use of technology or software; and

(5) Certain commodities produced by any plant or major component of a plant located outside the United States that is a direct product of U.S.-origin technology or software, as described in § 736.2(b)(3) of the EAR.

(b) The following items are not subject to the EAR:

(1) Items that are exclusively controlled for export or reexport by the following departments and agencies of the U.S. Government which regulate exports or reexports for national security or foreign policy purposes:

(i) Department of State. The International Traffic in Arms Regulations (22 CFR part 121) administered by the Office of Defense Trade Controls relate to defense articles and defense services on the U.S. Munitions List. Section 38 of the Arms Export Control Act (22 U.S.C. 2778).

(ii) Treasury Department, Office of Foreign Assets Control (OFAC). Regulations administered by OFAC implement broad controls and embargo transactions with certain foreign countries. These regulations include controls on exports and reexports to certain countries (31 CFR chapter V). Trading with the Enemy Act (50 U.S.C. app. section 1 et seq.), and International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.)

(iii) U.S. Nuclear Regulatory Commission (NRC). Regulations administered by NRC control the export and reexport of commodities related to nuclear reactor vessels (10 CFR part 110). Atomic Energy Act of 1954, as amended (42 U.S.C. part 2011 et seq.).

(iv) Department of Energy (DOE). Regulations administered by DOE control the export and reexport of technology related to the production of special nuclear materials (10 CFR part 810). Atomic Energy Act of 1954, as amended (42 U.S.C. section 2011 et seq.).

(v) Patent and Trademark Office (PTO). Regulations administered by PTO provide for the export to a foreign country of unclassified technology in the form of a patent application or an amendment, modification, or supplement thereto or division thereof (37 CFR part 5). BXA has delegated authority under the Export Administration Act to the PTO to approve exports and reexports of such technology which is subject to the EAR. Exports and reexports of such technology not approved under PTO regulations must comply with the EAR.

(2) Prerecorded phonograph records reproducing in whole or in part, the content of printed books, pamphlets, and miscellaneous publications, including newspapers and periodicals; printed books, pamphlets, and miscellaneous publications including bound newspapers and periodicals; children's picture and painting books; newspaper and periodicals, unbound, excluding waste; music books; sheet music; calendars and calendar blocks, paper; maps, hydrographical charts, atlases, gazetteers, globe covers, and globes (terrestrial and celestial); exposed and developed microfilm reproducing, in whole or in part, the content of any of the above; exposed and developed motion picture film and soundtrack; and advertising printed matter exclusively related thereto.

(3) Publicly available technology and software, except software controlled for EI reasons under ECCN 5D002 on the Commerce Control List, that:

(i) Are already published or will be published as described in § 734.7 of this part;

(ii) Arise during, or result from, fundamental research, as described in § 734.8 of this part;

(iii) Are educational, as described in § 734.9 of this part;

(iv) Are included in certain patent applications, as described in § 734.10 of this part.

Note to paragraphs (b)(2) and (b)(3) of this section: A printed book or other printed material setting forth encryption source code is not itself subject to the EAR (see § 734.3(b)(2)). However, notwithstanding § 734.3(b)(2), encryption source code in electronic form or media (e.g., computer diskette or CD ROM) remains subject to the EAR (see § 734.3(b)(3)).

(4) Foreign made items that have greater than the de minimis U.S. content based on the principles described in § 734.4 of this part.

(c) "Items subject to the EAR" consist of the items listed on the Commerce Control List (CCL) in part 774 of the EAR and all other items which meet the definition of that term. For ease of reference and classification purposes, items subject to the EAR which are not listed on the CCL are designated as "EAR99."

15 C.F.R. § 734.7 Published information and software.

(a) Information is "published" when it becomes generally accessible to the interested public in any form, including:

(1) Publication in periodicals, books, print, electronic, or any other media available for general distribution to any member of the public or to a community of persons interested in the subject matter, such as those in a scientific or engineering discipline, either free or at a price that does not exceed the cost of reproduction and distribution (See Supplement No. 1 to this part, Questions A(1) through A(6));

(2) Ready availability at libraries open to the public or at university libraries (See Supplement No. 1 to this part, Question A(6));

(3) Patents and open (published) patent applications available at any patent office; and

(4) Release at an open conference, meeting, seminar, trade show, or other open gathering.

(i) A conference or gathering is "open" if all technically qualified members of the public are eligible to attend and attendees are permitted to take notes or otherwise make a personal record (not necessarily a recording) of the proceedings and presentations.

(ii) All technically qualified members of the public may be considered eligible to attend a conference or other gathering notwithstanding a registration fee reasonably related to cost and reflecting an intention that all interested and technically qualified persons be able to attend, or a limitation on actual attendance, as long as attendees either are the first who have applied or are selected on the basis of relevant scientific or technical competence, experience, or responsibility (See Supplement No. 1 to this part, Questions B(1) through B(6)).

(iii) "Publication" includes submission of papers to domestic or foreign editors or reviewers of journals, or to organizers of open conferences or other open gatherings, with the understanding that the papers will be made publicly available if favorably received. (See Supplement No. 1 to this part, Questions A(1) and A(3)).

(b) Software and information is published when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution. See Supplement No. 1 to this part, Questions G(1) through G(3).

(c) Notwithstanding paragraphs (a) and (b) of this section, note that encryption software controlled under ECCN 5D002 for "EI" reasons on the Commerce Control List (refer to Supplement No. 1 to part 774 of the EAR) remains subject to the EAR even when publicly available.

15 C.F.R. § 734.8 Information resulting from fundamental research.

(a) Fundamental research. Paragraphs (b) through (d) of this section and § 734.11 of this part provide specific rules that will be used to determine whether research in particular institutional contexts qualifies as "fundamental research". The intent behind these rules is to identify as "fundamental research" basic and applied research in science and engineering, where the resulting information is ordinarily published and shared broadly within the scientific community. Such research can be distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary reasons or specific national security reasons as defined in § 734.11(b) of this part. (See Supplement No. 1 to this part, Question D(8)). Note that the provisions of this section do not apply to encryption software controlled under ECCN 5D002 for "EI" reasons on the Commerce Control List (refer to Supplement No. 1 to part 774 of the EAR).

(b) University based research.

(1) Research conducted by scientists, engineers, or students at a university normally will be considered fundamental research, as described in paragraphs (b) (2) through (6) of this section. ("University" means any accredited institution of higher education located in the United States.)

(2) Prepublication review by a sponsor of university research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers does not change the status of the research as fundamental research. However, release of information from a corporate sponsor to university researchers where the research results are subject to prepublication review, is subject to the EAR. (See Supplement No. 1 to this part, Questions D(7), D(9), and D(10).)

(3) Prepublication review by a sponsor of university research solely to ensure that publication would not compromise patent rights does not change the status of fundamental research, so long as the review causes no more than a temporary delay in publication of the research results.

(4) The initial transfer of information from an industry sponsor to university researchers is subject to the EAR where the parties have agreed that the sponsor may withhold from publication some or all of the information so provided. (See Supplement No. 1 to this part, Question D(2).)

(5) University based research is not considered "fundamental research" if the university or its researchers accept (at the request, for example, of an industrial sponsor) other restrictions

on publication of scientific and technical information resulting from the project or activity. Scientific and technical information resulting from the research will nonetheless qualify as fundamental research once all such restrictions have expired or have been removed. (See Supplement No. 1 to this part, Question D(7) and D(9).)

(6) The provisions of § 734.11 of this part will apply if a university or its researchers accept specific national security controls (as defined in § 734.11 of this part) on a research project or activity sponsored by the U.S. Government. (See Supplement No. 1 to this part, Questions E(1) and E(2).)

(c) Research based at Federal agencies or FFRDCs. Research conducted by scientists or engineers working for a Federal agency or a Federally Funded Research and Development Center (FFRDC) may be designated as "fundamental research" within any appropriate system devised by the agency or the FFRDC to control the release of information by such scientists and engineers. (See Supplement No. 1 to this part, Questions D(8) and D(11).)

(d) Corporate research.

(1) Research conducted by scientists or engineers working for a business entity will be considered "fundamental research" at such time and to the extent that the researchers are free to make scientific and technical information resulting from the research publicly available without restriction or delay based on proprietary concerns or specific national security controls as defined in § 734.11(b) of this part.

(2) Prepublication review by the company solely to ensure that the publication would compromise no proprietary information provided by the company to the researchers is not considered to be a proprietary restriction under paragraph (d)(1) of this section. However, paragraph (d)(1) of this section does not authorize the release of information to university researchers where the research results are subject to prepublication review. (See Supplement No. 1 to this part, Questions D(8), D(9), and D(10).)

(3) Prepublication review by the company solely to ensure that prepublication would compromise no patent rights will not be considered a proprietary restriction for this purpose, so long as the review causes no more than a temporary delay in publication of the research results.

(4) However, the initial transfer of information from a business entity to researchers is not authorized under the "fundamental research" provision where the parties have agreed that the business entity may withhold from publication some or all of the information so provided.

(e) Research based elsewhere. Research conducted by scientists or engineers who are not working for any of the institutions described in paragraphs (b) through (d) of this section will be treated as corporate research, as described in paragraph (d) of this section. (See Supplement No. 1 to this part, Question D(8).)

15 C.F.R. § 734.9 Educational information.

"Educational information" referred to in § 734.3(b)(3)(iii) of this part is not subject to the EAR if it is released by instruction in catalog courses and associated teaching laboratories of academic institutions. Dissertation research is discussed in § 734.8(b) of this part. (Refer to Supplement No. 1 to this part, Question C(1) through C(6)). Note that the provisions of this section do not apply to encryption software controlled under ECCN 5D002 for "EI" reasons on the Commerce Control List (refer to Supplement No. 1 to part 774 of the EAR).

15 C.F.R. § 742.15 Encryption items.

Encryption items can be used to maintain the secrecy of information, and thereby may be used by persons abroad to harm national security, foreign policy and law enforcement interests. As the President indicated in E.O. 13026 and in his Memorandum of November 15, 1996, export of encryption software, like export of encryption hardware, is controlled because of this functional capacity to encrypt information on a computer system, and not because of any informational or theoretical value that such software may reflect, contain, or represent, or that its export may convey to others abroad. For this reason, export controls on encryption software are distinguished from controls on other software regulated under the EAR.

(a) License requirements. Licenses are required for all destinations, except Canada, for ECCNs having an "EI" (for "encryption items") under the "Control(s)" paragraph. Such items include: encryption commodities controlled under ECCN 5A002; encryption software controlled under ECCN 5D002; and encryption technology controlled under ECCN 5E002. (Refer to part 772 of the EAR for the definition of "encryption items'). For encryption items previously on the U.S. Munitions List and currently authorized for export or reexport under a State Department license, distribution arrangement or any other authority of the State Department, U.S. persons holding valid USML licenses and other approvals issued by the Department of State prior to December 30, 1996 may ship remaining balances authorized by such licenses or approvals under the authority of the EAR by filing Shippers Export Declarations (SEDs) with District Directors of Customs, citing the provisions of this section effective on December 30, 1996 and the State Department license number. Such shipments shall be in accordance with the terms and conditions, including the expiration date, existing at the time of issuance of the State license. Violations of such authorizations, terms and conditions constitute violations of the EAR. Any reports required for distribution and other types of agreements previously authorized by the Department of State, valid prior to December 30, 1996, should be henceforth submitted to BXA at the following address: Office of Strategic Trade and Foreign Policy Controls, Bureau of Export Administration, Department of Commerce, 14th Street and Pennsylvania Ave., N.W., Room 2705, Washington, D.C. 20230.

(b) Licensing policy. The following licensing policies apply to items identified in paragraph (a) of this section. This section refers you to Supplements No. 4, No. 5, and No. 7 to this part 742. For purposes of these supplements, "products" refers to commodities and software. Except as otherwise noted, applications will be reviewed on a case-by-case basis by BXA, in conjunction with other agencies, to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests.

(1) Certain mass-market encryption software. Consistent with E.O. 13026 of November 15,

1996 (61 FR 58767), certain encryption software that was transferred from the U.S. Munitions List to the Commerce Control List pursuant to the Presidential Memorandum of November 15, 1996 may be released from "EI" controls and thereby made eligible for mass market treatment after a one-time review. To determine eligibility for mass market treatment, exporters must submit a classification request to BXA. 40-bit mass market encryption software may be eligible for a 7-day review process, and company proprietary software may be eligible for 15-day processing. Refer to Supplement No. 6 to part 742 and § 748.3(b)(3) of the EAR for additional information. Note that the one- time review is for a determination to release encryption software in object code only unless otherwise specifically requested. Exporters requesting release of the source code should refer to paragraph (b)(3)(v)(E) of Supplement No. 6 to part 742. If, after a one-time review, BXA determines that the software is released from EI controls, such software is eligible for all provisions of the EAR applicable to other software, such as License Exception TSU for mass-market software. If BXA determines that the software is not released from EI controls, a license is required for export and reexport to all destinations, except Canada, and license applications will be considered on a case-by-case basis.

(2) Key Escrow, Key Recovery and Recoverable encryption software and commodities. Recovery encryption software and equipment controlled for EI reasons under ECCN 5D002 or under ECCN 5A002, including encryption equipment designed or modified to use recovery encryption software, may be made eligible for license exception KMI after a one-time BXA review. License Exception KMI is available for all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan. To determine eligibility, exporters must submit a classification request to BXA. Requests for one-time review of key escrow and key recovery encryption items will receive favorable consideration provided that, prior to the export or reexport, a key recovery agent satisfactory to BXA has been identified (refer to Supplement No. 5 to part 742) and security policies for safeguarding the key(s) or other material/informationrequired to decrypt ciphertext as described in Supplement No. 5 to part 742 are established to the satisfaction of BXA and are maintained after export or reexport as required by the EAR. If the exporter or reexporter intends to be the key recovery agent, then the exporter or reexporter must meet all of the requirements of a key recovery agent identified in Supplement No. 5 to part 742. In addition, the key escrow or key recovery system must meet the criteria identified in Supplement No. 4 to part 742. Note that eligibility is dependent on continued fulfilment of the requirements of a key recovery agent identified in Supplement No. 5 to part 742. Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider requests for eligibility to export key recovery encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named, consistent with national security and foreign policy. When BXA approves such cases, exporters of products described in Supplement No. 4 to part 742 are required to furnish the name of an agent by December 31, 1998. Requests for one-

time review of recoverable products which allow government officials to obtain, under proper legal authority and without the cooperation or knowledge of the user, the plaintext of the encrypted data and communications will receive favorable consideration.

(3) Non-recovery encryption items up to 56-bit key length DES or equivalent strength supported by a satisfactory business and marketing plan for exporting recoverable items and services.

(i) Manufacturers of non-recovery encryption items up to 56-bit key length DES or equivalent strength will be permitted to export and reexport under the authority of License Exception KMI provided that the requirements and conditions of the License Exception are met. Exporters must submit a classification request for an initial BXA review of the item and a satisfactory business and marketing plan that explains in detail the steps the applicant will take during the two-year transition period beginning January 1, 1997 to develop, produce, and/or market encryption items and services with recoverable features. Manufacturers would commit to produce key recovery products. Others would commit to incorporate such products into their own products or services. Such efforts can include: the scale of key recovery research and development, product development, and marketing plans; significant steps to reflect potential customer demand for key recovery products in the firm's encryption-related business; and how soon a key recovery agent will be identified. Note that BXA will accept requests for classification of non-recoverable encryption items up to 56-bit key length DES or equivalent strength under this paragraph from distributors, re-sellers, integrators, and other entities that are not manufacturers of the encryption items. The use of License Exception KMI is not automatic; eligibility must be renewed every six months. Renewal after each six-month period will depend on the applicant's adherence to explicit benchmarks and milestones as set forth in the plan approved with the initial license classification and amendments as approved by BXA. This relaxation of controls and use of License Exception KMI will last through December 31, 1998. The plan submitted with classifications for the export of non-recoverable encryption items up to 56-bit key length DES or equivalent strength must include the elements in Supplement No. 7 to part 742.

(ii) BXA will make a determination on such classification requests within 15 days of receipt. Exports and reexports of non-recoverable encryption items up to 56-bit key length DES or equivalent strength will be authorized under the provisions of License Exception KMI, contingent upon BXA's review and approval of a satisfactory progress report related to the ongoing plan submitted by the applicant. The applicant must submit a letter to BXA every six months requesting approval of the progress report. Note that distributors, re- sellers, integrators, or other entities that are not manufacturers of the encryption items are permitted to use License Exception KMI for exports and reexports of such items only in instances where a classification has been granted to the manufacturer of the encryption items or a classification has been granted to the distributors, re-sellers, integrators, or other entities. The authority to so export or reexport will be for a time period ending on the same day the producer's authority to export or reexport ends.

(4) All other encryption items--

(i) Encryption licensing arrangement. Applicants may submit license applications for exports and reexports of certain encryption commodities and software in unlimited quantities for all destinations except, Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan. Applications will be reviewed on a case- by-case basis. Encryption licensing arrangements may be approved with extended validity periods specified by the applicant in block #24 on Form BXA-748P. In addition, the applicant must specify the sales territory and classes of end- users. Such licenses may require the license holder to report to BXA certain information such as item description, quantity, value, and end-user name and address.

(ii) Applications for encryption items not authorized under an encryption licensing arrangement. Applications for the export and reexport of all other encryption items will be considered on a case-by-case basis.

(5) Applications for encryption technology. Applications for the export and reexport of encryption technology will be considered on a case-by-case basis.

(c) Contract sanctity. Contract sanctity provisions are not available for license applications reviewed under this section.

(d) [Reserved]

15 C.F.R. § 744.9 Restrictions on technical assistance by U.S. persons with respect to encryption items.

(a) General prohibition. No U.S. person may, without a license from BXA, provide technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States of encryption commodities and software that, if of United States origin, would be controlled for "EI" reasons under ECCN 5A002 or 5D002. Note that this prohibition does not apply if the U.S. person providing the assistance has a license or is otherwise entitled to export the encryption commodities and software in question to the foreign person(s) receiving the assistance. Note in addition that the mere teaching or discussion of information about cryptography, including, for example, in an academic setting, by itself would not establish the intent described in this section, even where foreign persons are present.

(b) Definition of U.S. person. For purposes of this section, the term U.S. person includes:

(1) Any individual who is a citizen or permanent resident alien of the United States;

(2) Any juridical person organized under the laws of the United States or any jurisdiction within the United States, including foreign branches; and

(3) Any person in the United States.

(c) License review standards. Applications involving activities described in this section will be reviewed on a case-by-case basis to determine whether the activity is consistent with U.S. national security and foreign policy interests.

15 C.F.R. § 744.9 Restrictions on technical assistance by U.S. persons with respect to encryption items.

(a) General prohibition. No U.S. person may, without a license from BXA, provide technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States of encryption commodities and software that, if of United States origin, would be controlled for "EI" reasons under ECCN 5A002 or 5D002. Note that this prohibition does not apply if the U.S. person providing the assistance has a license or is otherwise entitled to export the encryption commodities and software in question to the foreign person(s) receiving the assistance. Note in addition that the mere teaching or discussion of information about cryptography, including, for example, in an academic setting, by itself would not establish the intent described in this section, even where foreign persons are present.

(b) Definition of U.S. person. For purposes of this section, the term U.S. person includes:

(1) Any individual who is a citizen or permanent resident alien of the United States;

(2) Any juridical person organized under the laws of the United States or any jurisdiction within the United States, including foreign branches; and

(3) Any person in the United States.

(c) License review standards. Applications involving activities described in this section will be reviewed on a case-by-case basis to determine whether the activity is consistent with U.S. national security and foreign policy interests.