974 F.Supp. 1288
United States District Court,
N.D. California.

Daniel J. BERNSTEIN, Plaintiff,

v.

UNITED STATES DEPARTMENT OF STATE, et al., Defendants.

No. C–95–0582 MHP.
Aug. 25, 1997.

Mathematician sought declaratory and injunctive relief against enforcement of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) on the ground that they were unconstitutional on their face and as applied to the mathematician's cryptographic computer source code. On cross-motions for summary judgment, the District Court, 945 F.Supp. 1279, invalidated parts of the regulations. Mathematician filed an amended complaint after a new executive order transferred regulatory authority to the Department of Commerce. On various motions, the District Court, Patel, J., held that: (1) there was no basis for a statutory, non-constitutional challenge to the executive order; (2) the encryption regulations issued by the Bureau of Export Administration (BXA) were directed quite specifically and "by their terms" to the entire field of applied scientific research and discourse and, thus, were subject to a facial prior restraint analysis, even though the export of commercial cryptographic software programs may not have been undertaken for expressive reasons; and (3) the regulations were unconstitutional prior restraints in violation of the First Amendment, inasmuch as encryption software was singled out and treated differently from other software regulated under the Export Administration Regulations (EAR). Ordered accordingly.

OPINION

PATEL, District Judge.

Plaintiff Daniel Bernstein originally brought this action against the Department of State and the individually named defendants seeking declaratory and injunctive relief from their enforcement of the Arms Export Control Act ("AECA"), 22 U.S.C. § 2778 (1990), and the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Pts. 120–30 (1994), on the grounds that they are unconstitutional on their face and as applied to plaintiff. The court granted in part and denied in part the parties' cross motions for summary judgment on December 9, 1996. Just prior to the court's order, President Clinton by Executive Order 13026 transferred jurisdiction over the export of nonmilitary encryption products to the Department of Commerce pursuant to the Export Administration Act of 1979 ("EAA"), 50 U.S.C.App. §§ 2401 *et seq.* (1991), and the Export Administration Regulations ("EAR"),

15 C.F.R. Pt. 730 *et seq.* (1997). On December 30, 1996, the Commerce Department issued an interim rule regulating the export of certain ***1292** encryption products. 61 Fed.Reg. 68572 (Dec. 30, 1996). Plaintiff subsequently amended his complaint to include the new regulations and new defendants. Now before this court are the parties' second cross-motions for summary judgment on the question of whether the licensing requirements for the export of cryptographic devices, software and related technology covered by the amendments to the EAR constitute an impermissible infringement on speech in violation of the First Amendment.

Having considered the parties' arguments and submissions, and for the reason set forth below, the court enters the following memorandum and order.

BACKGROUND[1]

At the time this action was filed, plaintiff was a PhD candidate in mathematics at University of California at Berkeley working in the field of cryptography, an area of applied mathematics that seeks to develop confidentiality in electronic communication. Plaintiff is currently a Research Assistant Professor in the Department of Mathematics, Statistics and Computer Science at the Encryption basically involves running a readable message known as University of Illinois at Chicago.

I. *Cryptography*

Encryption basically involves running a readable message known as “plaintext” through a computer program that translates the message according to an equation or algorithm into unreadable “ciphertext.” Decryption is the translation back to plaintext when the message is received by someone with an appropriate “key.” The message is both encrypted and decrypted by compatible keys.[2] The uses of cryptography are far-ranging in an electronic age, from protecting personal messages over the Internet and transactions on bank ATMs to ensuring the secrecy of military intelligence. In a prepublication copy of a report done by the National Research Council (“NRC”) at the request of the Defense Department on national cryptography policy, the NRC identified four major uses of cryptography: ensuring data integrity, authenticating users, facilitating nonrepudiation (the linking of a specific message with a specific sender) and maintaining confidentiality. Tien Decl., Exh. E, National Research Council, National Academy of Sciences, *Cryptograph's Role in Securing the Information Society* C–2 (Prepublication Copy May 30, 1996) (hereinafter “NRC Report”).

Once a field dominated almost exclusively by governments concerned with protecting their own secrets as well as accessing information held by others, the last twenty years has seen the popularization of cryptography as industries and individuals alike have increased their use of electronic media and have sought to protect their electronic products and communications. NRC Report at vii. As part of this transformation, cryptography has also become a dynamic academic discipline within applied mathematics. Appel Dec. at 5; Blaze Dec. at 2.

II. *Prior Regulatory Framework*

Plaintiff's original complaint and both of the court's decisions in this action were directed at the regulations in force at the time, the ITAR, promulgated to implement the AECA. The ITAR, administered within the State Department by the Director of the Office of Defense Trade Controls ("ODTC"), Bureau of Politico–Military Affairs, regulates the import and export of defense articles and defense services by designating such items to the United States Munitions List ("USML"). 22 U.S.C. § 2778(a)(1).[3] Items listed on the USML, which at the time included all cryptographic systems and software, require a license before they can be ***1293*** imported or exported. 22 U.S.C. § 2778(b)(2). The ITAR allows for a "commodity jurisdiction procedure" by which the ODTC determines if an article or service is covered by the USML when doubt exists about an item. 22 C.F.R. § 120.4(a).

As a graduate student, Bernstein developed an encryption algorithm he calls "Snuffle." He describes Snuffle as a zero-delay private-key encryption system. Complaint Exh. A. Bernstein has articulated his mathematical ideas in two ways: in an academic paper in English entitled "The Snuffle Encryption System," and in "source code" written in "C", a high-level computer programming language,[4] detailing both the encryption and decryption, which he calls "Snuffle.c" and "Unsnuffle.c", respectively. Once source code is converted into "object code," a binary system consisting of a series of 0s and 1s read by a computer, the computer is capable of encrypting and decrypting data.

In 1992 plaintiff submitted a commodity jurisdiction ("CJ") request to the State Department to determine whether Snuffle.c and Unsnuffle.c (together referred to as Snuffle 5.0), each submitted in C language source files, and his academic paper describing the Snuffle system, were controlled by ITAR.[5] The ODTC determined that the commodity Snuffle 5.0 was a defense article on the USML under Category XIII of the ITAR and subject to licensing by the Department of State prior to export. The ODTC identified the item as a "stand-alone cryptographic algorithm which is not incorporated into a finished software product." Complaint Exh. B.

Alleging that he was not free to teach, publish or discuss with other scientists his theories on cryptography embodied in his Snuffle program, plaintiff brought this action challenging the AECA and the ITAR on the grounds that they violated the First Amendment. In*Bernstein I* this court found that source code was speech for purposes of the First Amendment and therefore plaintiff's claims presented a colorable constitutional challenge and were accordingly justiciable. In *Bernstein II* the court concluded that the licensing requirements for encryption software under the ITAR constituted an unlawful prior restraint. The court also considered vagueness and overbreadth challenges to certain terms contained in the ITAR. The court issued its decision in *Bernstein II* on December 9, 1996.

III. *The Transfer of Jurisdiction and the Current Regulatory Framework*

On November 15, 1996, President Clinton issued Executive Order 13026, titled "Administration of Export Controls on Encryption Products," in which he ordered that jurisdiction over export controls on nonmilitary encryption products and related technology be transferred from the Department of State

to the Department of Commerce. The President's Executive Order specifies that encryption products that would be designated as defense articles under the USML and regulated under the AECA are now to be placed on the Commerce Control List ("CCL") under the EAR. The White House Press Release accompanying the Executive Order clarified that encryption products designed for military applications would remain on the USML and continue to be regulated under the ITAR. Press Release Accompanying Exec. Order No. 13026, at 2 (hereinafter "Press Release"). The Executive Order also provides a caveat that is repeated in the Press Release and throughout the new regulations: "the export of encryption software, like the export of other encryption products described in this section, must be controlled because of such software's functional capacity, ***1294** rather than because of any possible informational value of such software...." Exec. Order No. 13026, 61 Fed.Reg. 58768 (1996). The Press Release states that encryption products must be controlled for foreign policy and national security interests and concludes by noting that if the new regulations do not provide adequate controls on encryption products then such products will be redesignated as defense articles and placed again on the USML. Press Release, at 1, 4.

The EAR were promulgated to implement the EAA, but the EAA is not permanent legislation. Lapses in the EAA have been declared national emergencies and the President has issued Executive Orders authorizing continuation of the EAR export controls under the authority of the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701–1706. *See e.g.,* Exec. Order No. 12924, 59 Fed.Reg. 43437 (1994). Executive Order 13026 states that the authority of the President to administer these changes in the export control system under the EAR derives in part from the IEEPA and that the new controls on encryption products are "additional steps with respect to the national emergency described and declared" in the previous Executive Orders continuing in effect the EAR. Exec. Order No. 13026, 61 Fed.Reg. 58767 (1996).

On December 30, 1996, the Bureau of Export Administration ("BXA") under the Department of Commerce issued an interim rule amending the EAR "by exercising jurisdiction over, and imposing new combined national security and foreign policy controls on, certain encryption items that were on the [USML]." 61 Fed.Reg. 68572 (1996) (to be codified at 15 C.F.R. Pts. 730–774) ("encryption regulations" or "new regulations"). The EAR is structured around the CCL, 15 C.F.R. Pt. 774, 61 Fed.Reg. 12937 (1996), which categorizes items whose export is regulated according to various criteria, including the reason for their control. The new regulations add a category called "Encryption Items" or "EI" as a reason for control. 61 Fed.Reg. 68579 (1996) (to be codified at 15 C.F.R. § 738.2(d)(2)(I)(A)). Encryption items are defined as "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR." 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. § 772). This does not include those items still listed on the USML and controlled by the Department of State. With certain exceptions, one must obtain a license from the BXA prior to exporting any item listed on the CCL. See 15 C.F.R. Pts. 740–44. All items on the CCL

are given an Export Control Classification Number ("ECCN") which can be used to determine the categories under which an item is controlled and the reasons for its control.

The new regulations add three categories of items to the CCL which are controlled for EI reasons,[6] all of them more generally classified in Category 5, which covers telecommunications and information security. *See* 15 C.F.R. § 738.2(a). Those items are ECCN 5A002, covering encryption commodities; ECCN 5D002, covering encryption software; and ECCN 5E002, covering encryption technology. 61 Fed.Reg. 68586–87 (to be codified at 15 C.F.R. § 774 supp. I). For export licensing purposes, encryption software is treated the same as an encryption commodity. See note following ECCN 5D002. A commodity is defined generally as "[a]ny article, material, or supply except technology and software." 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. Pt. 772). Encryption software is regulated differently from other software controlled by the CCL and is defined as "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software." 61 Fed.Reg. 68585 (to be codified at 15 C.F.R. Pt. 772).[7] Definitions of ***1295** encryption source code and encryption object code have also been added.[8] Technology has not been amended by the encryption regulations and is defined generally as the technical data or technical assistance necessary for the development or use of a product. 15 C.F.R. Pt. 772. Controlled technology is that technology required for the development or use of items on the CCL. 15 C.F.R. Pt. 774 supp. 2 (General Technology Note). New restrictions on technical assistance have been added, however, to require a license to provide technical assistance (including training) to foreign persons with the intent to aid them in the foreign development of items that if they were domestic would be controlled under ECCNs 5A002 and 5D002.[9] 61 Fed.Reg. 68584 (to be codified at 15 C.F.R. § 744.9(a)); 61 Fed.Reg. 68579 (to be codified at 15 C.F.R. § 736.2(b)(7)(ii)).

The EAR defines export as "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...." 15 C.F.R. § 734.2(b)(1). The encryption regulations add a specific definition of export for encryption source code and object code software controlled under ECCN 5D002 which includes

downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the United States, over wire, cable, radio, electromagnetic, photooptical, photoelectric or other comparable communication 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.

61 Fed.Reg. 68578 (to be codified at 15 C.F.R. § 734.2(b)(9)).

A number of licensing exceptions are available under the EAR. *See* 15 C.F.R. Pt. 740. Under the encryption regulations, after a one-time review by BXA, licensing exceptions will be available for certain commercial encryption items, including mass-market encryption software, key-recovery software and commodities, and non-recovery encryption items up to 56–bit key length DES or equivalent strength software accompanied by a commitment to develop recoverable items. 61 Fed.Reg. 68581 (to be codified at 15 C.F.R. § 742.15). In general, items that are already publicly available or contain "de minimus" domestic content are not subject to the EAR. 15 C.F.R. §§ 734.3(b)(3) &734.4. However, as directed by the President and implemented by the new regulations, these exceptions do not apply to encryption commodities or software. 61 Fed.Reg. 68577–78 (to be codified at 15 C.F.R. §§ 732.2(b) & (d), 734.3(b)(3), 734.4(b)); Exec. Order No. 13026, 61 Fed.Reg. 58768 (1996) ("I have determined that the export of encryption products described in this section could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States ... "). This exception for encryption software to the general exclusion of publicly available items appears to pertain to publicly available or published information and software within the United States as well. 61 Fed.Reg. 68578 (to be codified at 15 C.F.R. § 734.7(c)). In addition, the EAR allows for broadly defined exceptions from the regulations for information resulting from fundamental research and educational information. 15 C.F.R. §§ 734.8, 734.9, & supp. 1. Neither ***1296** of these exceptions applies to encryption software controlled under ECCN 5D002. 61 Fed.Reg. 68579 (to be codified at 15 C.F.R. §§ 734.8, 734.9). They do appear to apply to encryption technology. Finally, phonographic records and most printed matter are not subject to the EAR and encryption software is not exempted from this exclusion. 15 C.F.R. § 734.3(b)(2). Indeed, an intriguing if somewhat baffling note appears in the new regulations: "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))."[10] 61 Fed.Reg. 68578 (to be codified at 15 C.F.R. § 734.3).

Licenses are required for export of items controlled by ECCNs 5A002, 5D002 and 5E002 for all destinations except Canada. 61 Fed.Reg. 68580 (to be codified at 15 C.F.R. § 742.15(a)). Applications for licenses "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." 61 Fed.Reg. 68581 (to be codified at 15 C.F.R. § 742.15(b)). The EAR provides that license applications will be resolved or referred to the President within 90 days. 15 C.F.R. § 750.4(a). While an applicant who is denied a license is informed of appeal procedures, 15 C.F.R. § 750.6(a)(6), the EAR does not appear to allow for judicial review. 15 C.F.R. § 756.2(c)(2); 50 U.S.C.App. § 2412(e).

LEGAL STANDARD

Under Federal Rule of Civil Procedure 56, summary judgment shall be granted "against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial ... since a complete failure of proof concerning an essential element of the nonmoving party's case necessarily renders all other facts immaterial."*Celotex Corp. v. Catrett,* 477 U.S. 317, 322–23, 106 S.Ct. 2548, 2552, 91 L.Ed.2d 265 (1986); *see also T.W. Elec. Serv. v. Pacific Elec. Contractors Ass'n,* 809 F.2d 626, 630 (9th Cir.1987) (the nonmoving party may not rely on the pleadings but must present significant probative evidence supporting the claim); *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 248, 106 S.Ct. 2505, 2510, 91 L.Ed.2d 202 (1986) (a dispute about a material fact is genuine "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.").

The court's function, however, is not to make credibility determinations, *Anderson,* 477 U.S. at 249, 106 S.Ct. at 2510–11, and the inferences to be drawn from the facts must be viewed in a light most favorable to the party opposing the motion. *T.W. Elec. Serv.,* 809 F.2d at 631.

Where as here, the question is purely a legal one involving no disputes of material fact, the matter is appropriately handled on a motion for summary judgment.

DISCUSSION

Plaintiff contends that the EAR, specifically the amendments regulating encryption items, both facially and as applied, constitutes a prior restraint on plaintiff's right to free speech, is unconstitutionally vague and overbroad, is content-based, and violates his freedom of association. Plaintiff also claims that the presidential transfer of jurisdiction to the Commerce Department and the encryption regulations themselves exceed their statutory authority and are ultra vires. Plaintiff requests declaratory and nationwide injunctive relief. In addition to opposing plaintiff's claims, defendants seek to dismiss certain defendants as extraneous and ask that the court vacate its decision in*Bernstein II.*

I. *Statutory Authority of the President and the Agency to Regulate Encryption Items*

1In his amended complaint plaintiff alleges that the presidential transfer of jurisdiction ***1297** and the subsequent agency regulations are ultra vires because the President and the Department of Commerce lacked statutory authority under the IEEPA to regulate encryption products. Plaintiff contends that the IEEPA, by its own terms, restricts the regulation of information protected by the First Amendment. Plaintiff also argues that use of the IEEPA requires an international emergency, which is not identified in the President's Executive Order. Plaintiff also maintains that the regulation of encryption products by the President and the Secretary violates the APA.

Defendants contend that the court lacks jurisdiction to review presidential determinations under the IEEPA. To the extent a claim may still lie against the Secretary, defendants argue that the IEEPA does not preclude export controls on encryption items.

Although the parties do not identify this claim as a threshold issue, plaintiff's argument is that the transfer of jurisdiction to Commerce and the Secretary's regulations were in excess of their statutory authority and are therefore invalid. To the extent this issue implicates the very validity of the current regulations, the court finds that it should be addressed before a review on the merits. In addition, courts must consider nonconstitutional questions before reaching constitutional considerations in order to avoid passing on constitutionality where possible. *Jean v. Nelson,* 472 U.S. 846, 854, 105 S.Ct. 2992, 2996–97, 86 L.Ed.2d 664 (1985).

A. *The IEEPA*

The IEEPA authorizes the President "to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat." 50 U.S.C. § 1701(a). Under this authority the President may "investigate, regulate, or prohibit any transaction in foreign exchange," 50 U.S.C. § 1702(a)(1)(A)(i), and "investigate, regulate, direct and compel, nullify, void, prevent or prohibit, any ... exportation of ... any property in which any foreign country or a foreign national thereof has any interest...." 50 U.S.C. § 1702(a)(1)(B). However, the IEEPA explicitly excludes any authority

to regulate or prohibit, directly or indirectly—any postal, telegraphic, or other personal communication, which does not involve a transfer of anything of value; ... or the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.

50 U.S.C. § 1702(b)(1) & (3) (1991 & Supp.1996). The statute goes on to limit the above exemption to those exports which are not otherwise controlled under sections 2404 and 2405 of the EAA. 50 U.S.C. § 1702(b)(3).

The IEEPA was passed in 1977 as a refinement of the Trading With the Enemy Act of 1917 ("TWEA"), which at the time provided a source of presidential emergency authority. S.Rep. No. 95–466, at 2 (1977), *reprinted in* 1977 U.S.C.C.A.N. 4540,4541. In the Senate Report accompanying the passage of the IEEPA, the Committee suggests that what became section 1702(b) was intended to exclude donations and humanitarian contributions from emergency regulation so long as such transfers did not subvert the effective exercise of emergency authority. S.Rep. No. 95–466, at 5 Section 1702(b)(3) of the IEEPA was enacted in 1988 and amended in 1994 to broaden and strengthen the exemption for informational materials. According to the House Conference Report, language adopted in 1988 was intended to ensure "that no embargo may prohibit or restrict directly or indirectly the import or export of information that is protected under the First Amendment to the

U.S. Constitution. The language was explicitly intended, by including the words 'directly or indirectly' to have a broad scope." H.R. Con. Rep. No. 103–482, at 239 (1994), *reprinted in* 1994 U.S.C.C.A.N. 302, 483. However, overly-narrow interpretations of section 1702(b)(3) by the Treasury Department prompted the 1994 amendment to "facilitate transactions and activities incident to ***1298** the flow of information and informational materials without regard to the type of information, its format, or means of transmission, and electronically transmitted information...." H.R. Con. Rep. No. 103–482, at 239.

B. *Statutory Authority of the President to Regulate Encryption Items Under the IEEPA*

2Plaintiff argues that President Clinton exceeded his authority under the IEEPA because the encryption items regulated are properly exempt from regulation under section 1702(b) and because the transfer was not a temporary exercise of emergency authority.[11]Defendants claim that the President's actions are not reviewable.

It is clear that the President's order is not reviewable under the APA. *Franklin v. Massachusetts,* 505 U.S. 788, 796, 112 S.Ct. 2767, 2773, 120 L.Ed.2d 636 (1992). In *Franklin,* an action seeking APA review of the decennial reapportionment of the House of Representatives, the Supreme Court concluded that "the final action complained of is that of the President, and the President is not an agency within the meaning of the [APA]." *Id.* The Court went on to note that the President's actions were still reviewable for constitutionality. *Id.* at 801, 112 S.Ct. at 2775–76.

3Less clear is the extent to which a court may review a non-APA claim that the President exceeded his statutory authority where there is no allegation of a constitutional violation. Not long after *Franklin* the Supreme Court decided *Dalton v. Specter,* 511 U.S. 462, 114 S.Ct. 1719, 128 L.Ed.2d 497 (1994), in which it reviewed a claim that the President exceeded his statutory authority under the Defense Base Closure and Realignment Act. The court below had attempted to follow Franklin by reasoning that when the President's actions exceed his statutory authority he also violates the constitutional separation of powers doctrine. *Id.* at 471, 114 S.Ct. at 1725. The *Dalton*Court rejected this conclusion, holding that "claims simply alleging that the President has exceeded his statutory authority are not 'constitutional' claims, subject to judicial review under the exception recognized in *Franklin." Id.* at 473–74, 114 S.Ct. at 1726–27(footnote omitted). However, the Court did not rule out the possibility of judicial review of statutory claims entirely.

We may assume for the sake of argument that some claims that the President has violated a statutory mandate are judicially reviewable outside the framework of the APA. But longstanding authority holds that such review is not available when the statute in question commits the decision to the discretion of the President.

Id. at 474, 114 S.Ct. at 1727 (citing *Dames & Moore v. Regan,* 453 U.S. 654, 667, 101 S.Ct. 2972, 2980, 69 L.Ed.2d 918 (1981)). The Court went on to conclude that the statute in question did not limit the President's discretion and was therefore unreviewable.

Notably, *Dames & Moore,* the case cited by the Court for the proposition that some non-APA statutory claims may still be subject to judicial review, involved review of various Executive Orders and regulations issued pursuant to the IEEPA which nullified attachments on Iranian assets in the United States and suspended claims against Iran following the hostage crisis. While the Court did not address the reviewability of the claims,[12] it did indicate that when the President acts under authorization from Congress "the executive action 'would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.' " *Dames & Moore,* 453 U.S. at 668, 101 S.Ct. at 2981 (quoting *Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579, 637, 72 S.Ct. 863, 871, 96 L.Ed. 1153 (1952)). The Court concluded that the IEEPA did authorize the nullification of attachments but did not directly authorize the suspension of claims. *Id.* at 675, 72 S.Ct. at 932–33. However, despite this conclusion,***1299*** the Court went on to find that due in part to the tenor and breadth of the IEEPA and congressional acquiescence in the practice of claim settlement by executive agreement, the President did not lack the power to settle claims against Iran.

Although the Supreme Court suggested the possibility of judicial review of non-APA statutory claims, it did not indicate, beyond the very narrow and specific instance identified in *Dames & Moore,* under what circumstances that review might take place. One appellate court has concluded that *Dalton* does not preclude judicial review of executive action for conformity with an authorizing statute, or any other statute. *Chamber of Commerce of U.S. v. Reich,* 74 F.3d 1322, 1331 (D.C.Cir.1996). Unlike the actions in *Franklin* and *Dalton* where the final action taken was by the President, and much like the present case, *Chamber of Commerce* involved an Executive Order which initiated agency regulations where the regulations carried direct and final consequences for the plaintiff. However, the court in *Chamber of Commerce* speaks boldly about the reviewability of executive action without readily distinguishing between whether such review lies equally for the President as for an executive official.[13] In fact, in a footnote the court concedes that the "*Dalton* Court's hesitancy to review presidential action ... suggests a reluctance to bring judicial power to bear directly on the President. Of course, here we are concerned with the long established non-statutory review of a claim directed at a subordinate executive official." *Id.* at 1331 n. 4. Indeed, the court goes on to note that in all the cases cited by the *Dalton* court, "special reasons existed for concluding that judicial review was precluded." *Id.* at 1331 n. 5. Those reasons involved matters of political discretion and national security. *Id.*

Finally, in *United States v. Spawr Optical Research, Inc.,* 685 F.2d 1076 (9th Cir.1982), the Ninth Circuit, in a case predating *Franklin* and*Dalton,* reviewed an Executive Order by President Ford

under the IEEPA's predecessor, the TWEA, continuing the EAA export regulations pending expiration of that Act. The Spawrs were convicted of the unlicensed exportation of laser mirrors after the EAA's expiration "when the sole basis for the regulations was the Executive Order." *Id.* at 1080. Much like plaintiff here, the Spawrs argued on appeal that the government lacked authority to prosecute them because there was no genuine emergency, the regulations were not related to any emergency then in effect, and Congress had intended to let the regulations lapse. *Id.* Reviewing language very similar to that of the IEEPA, the court found that the statute afforded broad and extensive powers. *Id.* Noting that in the face of such broad discretion, courts have been wary of reviewing the political considerations involved in declaring or continuing a national emergency, the*Spawr* court declined to do so as well. Id. However, the court then concluded that "[a]lthough we will not address these essentially-political questions, we are free to review whether the actions taken pursuant to a national emergency comport with the power delegated by Congress." *Id.* at 1081 (citing *United States v. Yoshida International, Inc.,* 63 C.C.P.A. 15, 526 F.2d 560, 579 (Cust. & Pat.App.1975)). In swift analysis the court went on to find that the regulations were rationally related to the emergency claimed and that Congress did not intend to terminate the regulations. *Id.* In fact, the court noted that each time the EAA had lapsed previously the President had issued an Executive Order declaring a national emergency to continue the export regulations and "Congress not only tolerated this practice, it expressed approval of the President's reliance on the TWEA to maintain the export regulations." *Id.* Such has been the case under the IEEPA as well.[14] *See, e.g.,* Exec. Order No. 12444, ***1300** 48 Fed.Reg. 48215 (1983); Exec. Order No. 12730, 55 Fed.Reg. 40373 (1990), reprinted in 50 U.S.C.App. § 1701 at 598 (1991); Exec. Order No. 12924, 59 Fed.Reg. 43437 (1994). Plaintiff notes that in recent years Congress has criticized use of the IEEPA to extend export regulations when the EAA lapses. Plf. Mem. in Opp. at 17 n. 49 (citing statements made by various members of Congress). Be that as it may, it is within Congress' power to change this practice and it has chosen not to.

While the analysis in *Spawr* is useful given that the facts are strikingly similar to the instant action, this court cannot ignore the skepticism with which the Supreme Court recently has approached judicial review of a presidential exercise of statutory authority absent a constitutional claim. As noted above, this case differs from *Franklin* and *Dalton* in that the final action is taken by the agency rather than the President.[15] But that does not significantly change the analysis of whether the actions the President took are reviewable. On this score *Chamber of Commerce* is not illuminating and the Supreme Court's allusion to *Dames & Moore* remains opaque. Indeed, given that the law is still unsettled on this question and that considerations precluding review do not apply to agencies—thereby allowing plaintiff to seek the same relief from agency action on the basis of a claim that the agency acted in excess of statutory authority—the court favors deference to the executive. In light of the recent Supreme Court decisions in this area, this court concludes that it cannot review whether

the President exceeded his statutory authority under the IEEPA to transfer jurisdiction of encryption items to the Commerce Department.

C. *Statutory Authority of the Commerce Secretary to Regulate Encryption Items Under the IEEPA*

Of critical importance in both *Franklin* and *Dalton* was the fact that the President was responsible for the final action under the statutes at issue. "What is crucial is the fact that '[t]he President, not the [Commission], takes the final action that affects' the military installations."*Dalton,* 511 U.S. at 470, 114 S.Ct. at 1725 (quoting *Franklin,* 505 U.S. at 799, 112 S.Ct. at 2774–75). Here we have the situation at issue in *Chamber of Commerce,* where the President's Executive Order initiated the regulatory process and left it to the agency to finalize the rules. "That the Secretary's regulations are based on the President's Executive Order hardly seems to insulate them from judicial review...." *Chamber of Commerce,* 74 F.3d at 1327; see also *Milena Ship Management Co. Ltd. v. Newcomb,* 804 F.Supp. 846, 850 (E.D.La.1992) (reviewing agency action taken pursuant to an unchallenged executive order under the IEEPA). Accordingly, this court will examine whether the Commerce Department's regulation of encryption items is consistent with the IEEPA.[16]

4To the extent that plaintiff argues that the regulations governing encryption are not a temporary exercise of emergency power, the question really belongs to the legitimacy of the Executive Order in the first instance and the court declines to address it. The declaration of a national emergency is an action that rests with the President and is based on his broad discretion under section 1701 of the IEEPA. Moreover, the question of employing the IEEPA—or the TWEA before it—to maintain export regulations during lapses in the EAA was essentially laid to rest by the Ninth Circuit in *Spawr* and by the legislative history of the IEEPA.

***1301** [I]t is unmistakable that Congress intended to permit the President to use the TWEA to employ the same regulatory tools during a national emergency as it had employed under the EAA. We, therefore, conclude that the President had the authority during the nine-month lapse in the EAA to maintain the export regulations.

Spawr, 685 F.2d at 1082.

5The gravamen of plaintiff's ultra vires argument is that the IEEPA does not authorize the regulation of speech, particularly speech that does not involve a foreign interest in property, and that as speech, encryption software fits well within the exemption for personal communications and informational materials in sections 1702(b)(1) & (3).

With respect to whether encryption software fits within the scope of "property in which any foreign country or a national thereof has any interest", the court finds that section 1702(a)(1) is sufficiently broad to allow for many forms of property, both tangible and intangible, and many forms of interest, both direct and indirect. *See* 31 C.F.R. §§ 500.311, 500.312; *see also Spawr,* 685 F.2d at 1081 n.

10 (finding that section 5(b) of the TWEA was broad enough to allow regulation “of any property to any foreign country”). Encryption software or other technology comes within this section.

6Plaintiff also alleges that the regulations are beyond the statutory authority of the IEEPA because they affect personal communications and informational materials. Section 1702(b)(1) prohibits direct or indirect regulation of “any postal, telegraphic, telephonic or other personal communication” which does not transfer anything of value. As defendants convincingly argue, to the extent this argument is directed at academic discussion of cryptographic ideas, the regulations attempt to exempt such communications—although whether they do so according to the demands of the First Amendment is a separate question. To the extent this argument is directed at cryptographic software generally, it does not appear to fit within this seemingly narrow and simple provision. Nor can it be assured that software would have no value. Indeed, there are potentially billions of dollars at stake in the export of commercial encryption software. *See* Jared Sandberg, “Judge Rules Encryption Software Is Speech in Case on Export Curbs,” Wall St. J., Apr. 18, 1996, at B7. Thus, the regulations do not exceed this statutory provision.

7Finally, plaintiff contends that the regulations go beyond the authority provided by section 1702(b)(3) which specifically limits regulation of information or informational materials regardless of format or medium of transmission. Plaintiff argues that the broad scope of this provision precludes regulation of encryption software. In addition, plaintiff contends that by specifically referencing sections 2404 and 2405 of the EAA, and exempting—from the informational materials exemption—items “otherwise controlled for export” under those sections, the court is bound by principles of statutory construction to consider only those items controlled when section 1702(b)(3) was last amended, or April 30, 1994. Plaintiff then concludes that because encryption software fits within the scope of this provision and was not otherwise controlled under the EAA as of April of 1994, it cannot be regulated under the IEEPA.

Defendants contend that section 1702(b)(3) does not expressly provide for software, and that to include software in those items exempted from regulation for their informational value would lead to absurd results. Moreover, defendants counter plaintiff's statutory construction argument and claim that the items exempted from this provision by virtue of being controlled under the EAA are not only those that were on the Commerce Control List as of April of 1994 but any others that have since been added—including the encryption technology at issue here. Defendants also argue that to read section 1702(b)(3) as exempting encryption software on the basis that it is protected under the First Amendment would be to impose a novel theory of free speech not contemplated by Congress. As noted above, the IEEPA explicitly excludes any authority

“to regulate or prohibit, directly or indirectly—... the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless ***1302** of format or medium of transmission, of any information or informational materials, including but not limited to, publications,

films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 2404 of the Appendix to this title, or under section 2405 of the Appendix to this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States...."

50 U.S.C. § 1702(b)(3) (Supp.1996).

First, the court must consider whether software—in this case, encryption software—comes within the exception to the exception; if so, then the instant regulations do not exceed their statutory authority. In other words, anything controlled by sections 2404 and 2405 of the EAA may be regulated regardless of its informational content. Under the referenced sections of the EAA the President may "prohibit or curtail the exportation of any goods, technology, or other information subject to the jurisdiction of the United States" for either national security or foreign policy reasons. 50 U.S.C.App. § 2405(a)(1) (foreign policy controls); 50 U.S.C.App. § 2404(a)(1) (national security controls). It is not disputed that Executive Order 13026, by transferring encryption products to the Commerce Control List ("CCL"), subjected them to regulation under sections 2404 and 2405 of the EAA.

The question becomes whether reference to sections 2404 and 2405 of the EAA should be understood to include all items currently on the CCL—in which case the present regulations effectively remove encryption products from the exemption—or whether rules of statutory construction require the court to construe the reference to those sections as including only those items listed at the time section 1702(b) was last amended, or April 30, 1994. A secondary issue complicates this already complicated matter further: since sections 2404and 2405 do not themselves designate specific items on the CCL, which is governed by regulation, does the construction of the IEEPA with respect to those sections also apply to their implementing regulations?

Plaintiff relies on a canon of statutory construction discussed in *Hassett v. Welch,* 303 U.S. 303, 314, 58 S.Ct. 559, 564–65, 82 L.Ed. 858 (1938) and *Pearce v. Director, Office of Workers' Comp. Programs,* 603 F.2d 763, 767 (9th Cir.1979) which holds that without clear congressional indication to the contrary, where one statute adopts provisions of another by specific reference to the provisions adopted (known as a statute of specific reference) the effect is that such adoption takes the provision as it existed at the time of adoption and does not include subsequent amendments; conversely, where a statute adopts the general law in a given area (a statute of general reference), it is construed to adopt that law's subsequent amendments. *See* 2A Sutherland, Statutory Construction § 51.07 (4th ed.1984). Plaintiff claims that the IEEPA is a statute of specific reference and cannot be read as adopting subsequent changes to sections 2404 and 2405 of the EAA. Plaintiff further supports this position by pointing to the fact that at least one agency has interpreted the "informational materials" provision to exclude items that were, as of April 30, 1994, controlled for

export under sections 5 and 6 of the EAA. 31 C.F.R. § 560.315(b) (Office of Foreign Assets Control regulation of Iranian transactions).

Defendants contend that the IEEPA is more like the statute in *United States v. Smith,* 683 F.2d 1236 (9th Cir.1982), in which the Ninth Circuit read the Youth Corrections Act ("YCA") as not incorporating specific provisions of the general probation statute. The court concluded that while there were persuasive arguments on both sides, the YCA did not really appear to adopt or incorporate the referenced provisions of the probation statute. "Rather, it merely provides that the YCA is not to 'be construed in any wise to amend, repeal, or affect the provisions of' the probation statute." *Id.* at 1239. According to the court this was not properly a statute of specific reference in which certain provisions of another statute are incorporated into it, but one that "actually emphasizes that these are distinct statutes". *Id.* Under defendants' reasoning, ***1303** section 1702(b)(3) of the IEEPA does not incorporate sections 2404 and 2405 of the EAA but rather distinguishes them and as such those sections are to be read with their full and current force.

This court believes that defendants have the better argument. The rules of statutory interpretation are not hard and fast. "A provision which, in terms, however, reads as a specific reference may, in context, be construed as a general reference." *United States v. Rodriguez–Rodriguez,* 863 F.2d 830, 831 (11th Cir.1989). Such is the case here. Read in context, section 1702(b)(3) *excludes* rather than incorporates those items covered under the EAA. Moreover, the sections referenced are themselves fairly general and are clearly intended to be fleshed out by regulations suited to meet the changing needs of national security and foreign policy. Given the goals of the IEEPA and the powers it gives the President, it would seem odd indeed for Congress to exclude from the exemption those items the President deems sensitive to the national security under the EAA, but to freeze that list of items as of a certain date. As the court noted in Smith, this "is the more appropriate interpretation in view of the policies that the [statute] is designed to advance. It is proper, and indeed essential, to interpret the words of a statute in the light of the purposes Congress was seeking to serve." 683 F.2d at 1240 (citations omitted). Therefore, because encryption products are currently regulated under sections 2404 and 2405 of the EAA they do not fall within the exemption for informational materials.[17]

8Accordingly, this court finds that the regulation of encryption items is not prohibited by section 1702(b)(3) and therefore does not exceed the statutory authority provided by the IEEPA. It is worth noting at this juncture that this court's rather narrow determination that source code is speech protected by the First Amendment does not serve to remove encryption technology from all government regulation. Both parties exaggerate the debate needlessly. Plaintiff does so by aggrandizing the First Amendment, by assuming that once one is dealing with speech that it is immaterial what the consequences of that speech may be. Defendants do so by minimizing speech, by constantly referring to "mere speech" or "mere ideas" in their briefs and assuming that the

functionality of speech can somehow be divorced from the speech itself. This controversy is before this court precisely because there is no clear line between communication and its consequences. While defendants may have the authority to regulate encryption source code, they must nonetheless do so within the bounds of the First Amendment.

II. *Prior Restraint*[18]

A. *Analytical Framework*

9As the Supreme Court has stated, in determining the extent of the constitutional protection afforded by the guarantees of the First Amendment, "it has been generally, if not universally, considered that it is the chief purpose of the guaranty to prevent previous restraints upon publication." *Near v. Minnesota,* 283 U.S. 697, 713, 51 S.Ct. 625, 630, 75 L.Ed. 1357 (1931). It is for this reason that the Court has held: "Any prior restraint on expression comes to this Court with a 'heavy presumption' against its constitutional validity." *Organization for a Better Austin v. Keefe,* 402 U.S. 415, 419, 91 S.Ct. 1575, 1578, 29 L.Ed.2d 1 (1971) (citations omitted).

10While prior restraints have often come in the form of judicial injunctions on publication, see *e.g., C.B.S. v. Davis,* 510 U.S. 1315, 114 S.Ct. 912, 127 L.Ed.2d 358 (1994); *New York Times Co. v. United States,* 403 U.S. 713, 91 S.Ct. 2140, 29 L.Ed.2d 822 (1971), they are also recognized in licensing schemes. *See e.g., FW/PBS, Inc. v. Dallas,* 493 U.S. 215, 110 S.Ct. 596, 107 L.Ed.2d 603 (1990); ***1304***Lakewood v. Plain Dealer Publishing Co.,* 486 U.S. 750, 108 S.Ct. 2138, 100 L.Ed.2d 771 (1988). Governments may impose valid time, place and manner restrictions when they are content neutral, narrowly tailored to serve a substantial governmental interest, and leave open alternative channels for communication. *See e.g., Clark v. Community for Creative Non–Violence,* 468 U.S. 288, 293, 104 S.Ct. 3065, 3068–69, 82 L.Ed.2d 221 (1984). However, "even if a government may constitutionally impose-content-neutral prohibitions on a particular manner of speech, it may not *condition* that speech on obtaining a license or permit from a government official in that official's boundless discretion." *Lakewood,* 486 U.S. at 764, 108 S.Ct. at 2147.

11It is axiomatic that the First Amendment is more tolerant of subsequent criminal punishment of speech than it is of prior restraints on the same speech.

The thread running through all these cases is that prior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights. A criminal penalty or a judgment in a defamation case is subject to the whole panoply of protections afforded by deferring the impact of the judgment until all avenues of appellate review have been exhausted .....

A prior restraint, by contrast and by definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanction after publication "chills" speech, prior restraint "freezes" it at least for the time.

Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559, 96 S.Ct. 2791, 2802–03, 49 L.Ed.2d 683 (1976).

12While the Supreme Court has consistently rejected the idea that a prior restraint can never be employed, id. at 570, 96 S.Ct. at 2808, it nonetheless begins with a presumption of invalidity. The danger inherent in prior restraints is largely procedural, in that they bypass the judicial process and locate in a government official the delicate responsibility of passing on the permissibility of speech. *See**Freedman v. Maryland,* 380 U.S. 51, 58, 85 S.Ct. 734, 738, 13 L.Ed.2d 649 (1965) (holding that "a noncriminal process which requires the prior submission of a film to a censor avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system".) Freedman sets forth three procedural safeguards that have been used by the Supreme Court to examine licensing schemes: 1) any restraint prior to judicial review can only be imposed for a brief and specified period during which the status quo prevails; 2) expeditious judicial review must be available; and 3) the censor must bear the burden of going to court to suppress speech and once there bears the burden of proof. *FW/PBS,* 493 U.S. at 227, 110 S.Ct. at 605–06 (citing *Freedman,* 380 U.S. at 58–60, 85 S.Ct. at 738–39).

13When the risks associated with unbridled licensing schemes are present to a significant degree, "courts must entertain an immediate facial attack on the law." *Lakewood,* 486 U.S. at 759, 108 S.Ct. at 2145.

B. *Analysis*

In *Bernstein II* this court held that the ITAR effected an unconstitutional prior restraint on speech due to inadequate procedural safeguards. Plaintiff contends that the new encryption regulations suffer from identical deficiencies. Defendants do not argue that the effect of the new regulations is notably different from that of the ITAR.[19] They do, however, present arguments against some of the reasoning in *Bernstein II* and to the extent that these arguments are applicable to the current analysis, the court will address them.

1. *Controls on Encryption Commodities and Software*

14First, defendants protest that a facial challenge is not applicable here because there is not a "close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of identified censorship risks." *Lakewood,* 486 U.S. at 759, 108 S.Ct. at 2145. In ***1305** *Lakewood,* a newspaper challenged a city ordinance which required annual permits for newsracks on public property and gave the mayor authority to grant or deny applications for those permits. The Court contrasted laws that are directed at expression, such as one governing the circulation of newspapers, with laws of general applicability not aimed at conduct commonly associated with expression, such as a law requiring building permits. *Id.* at 760–61, 108 S.Ct. at 2145–46. The former risks self-censorship on the part of those applying for permits and censorship on the part of the decisionmaker. The latter rarely do. *See also* *Freedman,* 380 U.S. 51, 85 S.Ct. 734, 13 L.Ed.2d 649 (licensing of films); *FW/PBS,* 493 U.S. 215, 110 S.Ct. 596, 107 L.Ed.2d 603(licensing of sexually-oriented businesses). Defendants contend that while licensing schemes

that vest unbridled discretion to regulate conduct commonly associated with expression are appropriate for facial attack under prior restraint doctrine, such is not the case here where the activity at issue is the programming of a computer to encrypt information.[20] Defendants also cite *Roulette v. City of Seattle,* 97 F.3d 300, 305 (9th Cir.1996), to support their contention that only laws narrowly and specifically directed at expressive activities are subject to facial challenge. At issue in *Roulette* was an ordinance that prohibited people from sitting or lying on public sidewalks in certain areas and during certain times. The court, in a pithy opinion, held that "[t]he fact that sitting can possibly be expressive, however, isn't enough to sustain plaintiffs' facial challenge to the Seattle ordinance.... Consistent with this speech-protective purpose, the Supreme Court has entertained facial freedom-of-expression challenges only against statutes that, 'by their terms,' sought to regulate" words or expressive conduct. *Id.* at 303 (quoting *Broadrick v. Oklahoma,* 413 U.S. 601, 612–13, 93 S.Ct. 2908, 2915–16, 37 L.Ed.2d 830 (1973)).

The court does not disagree with defendants' statement of the law but with their application to the facts. The encryption regulations issued by the BXA are much more like the regulation of newspaper racks than lying or sitting. The new regulations are directed quite specifically and "by their terms" to an entire field of applied scientific research and discourse. Where one places a newspaper rack is not an activity associated with expression, but the availability of newspapers generally is. Similarly, while the export of a commercial cryptographic software program may not be undertaken for expressive reasons, that same activity—undisputably regulated under the EAR—is often undertaken by scientists for purely expressive reasons. By the very terms of the encryption regulations, the most common expressive activities of scholars—teaching a class, publishing their ideas, speaking at conferences, or writing to colleagues over the Internet—are subject to a prior restraint by the export controls when they involve cryptographic source code or computer programs. In the field of applied science ideas are not just expressed in abstract, theoretical terms, but in precise applications. Those applications are subject to licensing under the encryption regulations and are excluded from the exemptions for fundamental research and educational information. This is precisely the kind of law identified in *Lakewood* that risks self-censorship on the part of those that must apply for licenses and censorship on the part of the decisionmaker. As the American Association for the Advancement of Science ("AAAS") stated to the BXA in their comments regarding the new regulations, the "basic thrust" of the Interim Rule

***1306** threatens to undermine essential features of scientific freedom and the open exchange of information that are generally acknowledged as critical to innovation in science and technology and are responsible in large part for the preeminence of America's research and development enterprise. AAAS opposes attempts by the government to restrict the communication or publication of unclassified research and technical information, efforts which we believe are inconsistent with scientific advancement.

Wimberly Decl., Exh. A, at 1. The regulations merit the application of the prior restraint doctrine because they present "a danger of unduly suppressing protected expression." *Freedman,* 380 U.S. at 54, 85 S.Ct. at 737.

15The encryption regulations, like Category XIII of the USML, is specifically directed at speech protected by the First Amendment. The Department of Commerce requires a license to export items controlled under ECCNs 5A002 and 5D002. And as made explicit by the new regulations, export includes publication where publication is or could be made electronic and even where the information to be published is already publicly available. In fact, in spite of the disclaimers regarding functionality and the exception for printed materials, the encryption regulations issued by the BXA appear to be even less friendly to speech interests than the ITAR. Here encryption software is singled out and treated differently than other software regulated under the EAR. 61 Fed.Reg. 68580 (to be codified at 15 C.F.R. § 742.15); *see FW/PBS,* 493 U.S. at 225, 110 S.Ct. at 604–05 ("Therefore, even assuming the correctness of the city's representation of its 'general' inspection scheme, the scheme involved here is more onerous with respect to sexually-oriented businesses than with respect to the vast majority of other businesses.").

And the exception for printed materials, while at first glance a concession to the speech interests involved, is so irrational and administratively unreliable that it may well serve to only exacerbate the potential for self-censorship. 61 Fed.Reg. 68578 (to be codified at15 C.F.R. § 734.3). First, the exception is unreliable because the BXA has indicated that it reserves the right to control scannable source code in printed form. 61 Fed.Reg. 68575. Second, the exception seeks to codify a distinction between paper and electronic publication that makes little or no sense and is untenable. *See Bernstein II,* 945 F.Supp. at 1291 n. 10. As the AAAS commented,

[w]hile it is acceptable under this provision to publish such material in a book and distribute it internationally without an export license, putting the same information on a disk and sending it abroad is subject to EAR approval. This distinction has serious ramifications for scholarly communication as many professional journals are now moving onto the Internet as electronic publications.

Wimberly Decl., Exh. A, at 1. As an example, the AAAS noted that their journal *Science* is available in both print and electronic form. At oral argument defendants admitted that encryption code in print form could be converted into a functioning encryption product, but defended the distinction on the basis that converting the print version to working software required a good deal of skill. The court is somewhat confounded by this explanation. Defendants claim that encryption poses unique and serious threats to national security, yet the printed matter exception belies this rationale by making encryption freely available to only those foreigners who are technologically sophisticated. Defendants conceded at oral argument that the effect of this dichotomy would be to make it more

difficult only for the more inept. This seems to defeat the very purpose of the regulation since those who likely pose a greater threat to national security are likely more willing to expend the time and resources in that effort and will not be prevented by the regulation. In effect, the exception undermines the stated purpose of the regulations. Again, the government conceded that in only a slightly greater length of time and with some greater technological skill, the regulation could be defeated.

Finally, the Supreme Court's recent decision in *Reno v. American Civil Liberties Union,* 521 U.S., 844, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997), suggests that not only is ***1307** the distinction between print and electronic media increasingly untenable, but that the Internet is subject to the same exacting level of First Amendment scrutiny as print media.

This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, 'the content on the Interact is as diverse as human thought.' We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

Id. at ——, 117 S.Ct. at 2344. Thus, the dramatically different treatment of the same materials depending on the medium by which they are conveyed is not only irrational, it may be impermissible under traditional First Amendment analysis.

As this court noted in *Bernstein II,* that BXA regulates encryption in the interest of national security does not alone justify a prior restraint.*In New York Times Co.,* 403 U.S. at 714, 91 S.Ct. at 2141–42, the Supreme Court invalidated a prior restraint on classified material that had been enjoined in the interests of national security. While that case inspired nine separate opinions on the propriety of enjoining publication of the Pentagon Papers in The New York Times and The Washington Post, a majority of Justices found national security, without more, too amorphous a rationale to abrogate the protections of the First Amendment. *See id.* at 719, 91 S.Ct. at 2144 (Black, J. and Douglas, J., concurring). Justice Brennan concluded that the First Amendment's ban on prior restraints could only be overridden in time of war, *id.* at 726, 91 S.Ct. at 2147–48 (Brennan, J. concurring) (citing *Schenck v. United States,* 249 U.S. 47, 39 S.Ct. 247, 63 L.Ed. 470 (1919)), and even then, according to Justice Stewart, only when disclosure would "surely result in direct, immediate, and irreparable damage to our Nation or its people." *Id.* at 730, 91 S.Ct. at 2149 (Stewart, J. and White, J. concurring). Even without a consensus from the Supreme Court on how exacting the standard should be, it is clear from *New York Times* that national security alone is insufficient without more. Yet that is exactly what both the President and the BXA have offered here as the justification for the

regulation: national security and foreign policy interests. Exec. Order No. 13026, 61 Fed.Reg. 58767; 61 Fed.Reg. 68573. Particularly now, when none of the encryption items subject to export controls under the EAR have military applications, a less amorphous rationale is required.[21]

16Nor is it necessary that an item be regulated for its content to make the regulations function as a prior restraint on speech. It is enough that they are directed at expressive activity. As the plurality opinion in *FW/PBS* suggests, even a licensing scheme with a content-neutral purpose must still contain adequate procedural safeguards in order to be constitutional.[22] Thus, without deciding whether the regulations are content-based, the court turns to the procedural safeguards afforded under the encryption regulations. As noted above, the Court in *FW/PBS* ****1308*** read Freedman to hold that for a licensing scheme to be constitutional, 1) the licensor must make the licensing decision within a specific and reasonable period of time; 2) there must be prompt judicial review; and 3) the censor must bear the burden of going to court to uphold a licensing denial and once there bears the burden of justifying the denial. *FW/PBS,* 493 U.S. at 227–28, 110 S.Ct. at 605–06 (citing *Freedman,* 380 U.S. at 58–60, 85 S.Ct. at 738–40). The new regulations, like the ITAR, are woefully inadequate.

17The EAR provides that license applications will be resolved or referred to the President within 90 days.[23] 15 C.F.R. § 750.4(a). However, there is no time limit on an application that has been referred to the President. If a license is denied, the agency provides an internal appeals process, 15 C.F.R. Pt. 756, but the only time limit on the appeals decision is that the agency "shall decide an appeal within a reasonable time after receipt of the appeal." 15 C.F.R. § 756.2(c)(1). That decision is final and not subject to judicial review. 15 C.F.R. § 756.2(c)(2); 50 U.S.C.App. § 2412(e); *see also United States v. Bozarov,* 974 F.2d 1037, 1044–45 (9th Cir.1992) (EAA's preclusion of judicial review does not violate nondelegation doctrine), *cert. denied,* 507 U.S. 917, 113 S.Ct. 1273, 122 L.Ed.2d 668 (1993).[24] And most important, and most lacking, are any standards for deciding an application. The EAR reviews applications for licenses "on a case-by-case basis" and appears to impose no limits on agency discretion. 61 Fed.Reg. 68581 (to be codified at 15 C.F.R. § 742.15(b)). Like the ordinance in *Lakewood,* where the mayor could deny a permit without any more justification than that it was not in the public interest, nothing in the regulations prevents the BXA from justifying a denial of an application by stating that it is contrary to national security and foreign policy interests.[25] As the Court noted in Lakewood, these are illusory constraints. 486 U.S. at 769, 108 S.Ct. at 2150–51; *see also Desert Outdoor Advertising Inc. v. City of Moreno Valley,* 103 F.3d 814, 818 (9th Cir.1996) (finding billboard permit requirement unconstitutional because city officials had "discretion to deny a permit on the basis of ambiguous and subjective reasons"). This court has stated previously that while it is mindful of the problems inherent in judicial review of licensing decisions regarding cryptographic software, both with respect to the sophistication of the technology and the potentially classified nature of the licensing considerations, there must still be some review available

if the export controls on cryptographic software are to survive the presumption against prior restraints on speech. In this case, for the reasons enumerated, the court concludes that the encryption regulations are an unconstitutional prior restraint in violation of the First Amendment.

2. *Controls on Encryption Technology*

Plaintiff does not distinguish the regulation of encryption technology—as opposed to commodities and software—for the purposes of prior restraint analysis. With respect to vagueness, the only provision he addresses as vague is "technical assistance." 15 C.F.R. § 744.9(a). Defendants allege that plaintiff lacks standing to challenge the controls on technology because they have not been applied to him and any injury is speculative. ***1309** Even if plaintiff is found to have standing,— defendants contend that a facial challenge is still inappropriate because *United States v. Edler Indus., Inc.,* 579 F.2d 516, 520 (9th Cir.1978), found that the technical data provisions of the predecessor to the AECA survived constitutional challenge with a narrowing construction.

18It does not appear necessary to address the vagueness argument advanced by plaintiff, or any of the other constitutional arguments, as the bulk of the encryption regulations have been adjudged to constitute a prior restraint on speech. The First Amendment does not "render inapplicable the rule that a federal court should not extend its invalidation of a statute further than is necessary to dispose of the case before it." *Brockett v. Spokane Arcades, Inc.,* 472 U.S. 491, 502, 105 S.Ct. 2794, 2801, 86 L.Ed.2d 394 (1985)(citation omitted). The restrictions on technical assistance under the new regulations prohibit a person from providing technical assistance without a license 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." 61 Fed.Reg. 68584 (to be codified at 15 C.F.R. § 744.9). The technical assistance provision also states that the "mere teaching or discussion of information about cryptography" does not establish the requisite intent. 61 Fed.Reg. 68584 (to be codified at 15 C.F.R. § 744.9(a)). However cryptic this provision might be viewed in relation to the more expansive exemptions for educational information and fundamental research elsewhere in the regulations, because it is dependent on the definitions and regulation of encryption commodities and software, it is unenforceable under the court's holding above.

III. *Proper Defendants*

19Plaintiff named three additional defendants in his supplemental complaint—the Departments of Energy ("DOE") and Justice ("DOJ") and the Central Intelligence Agency ("CIA")—because officials from each are now involved in some way with licensing reviews.61 Fed.Reg. 68585 (to be codified at 15 C.F.R. § 750.3(b)(2)(v)); 15 C.F.R. § 750.4(d)–(e); 15 C.F.R. § 772 (listing committees involved in interagency review and their members). Plaintiff also contends that these agencies are involved with overall jurisdictional decisions as well. Press Release, at 4 (stating that after legislative reauthorization of export controls the Secretaries of Defense and State together with the Attorney

General “shall reexamine whether adequate controls on encryption products can be maintained under the provisions of the new statute and advise the Secretary of Commerce of their conclusions as well as any recommendations for action”). Defendants claim that there is no justification for joining every agency that participates in the review process and that the Secretary of Commerce is the only proper defendant.

The court is inclined to agree with defendants. The roles played by the DOE, DOJ and the CIA are limited to consulting and advising the Secretary of Commerce who is responsible for final decisions. Even if those agencies are asked to review any new legislation that may be passed,[26] their roles are advisory. Accordingly, any determination against the Secretary of Commerce is sufficient and the DOE, DOJ and the CIA are dismissed as defendants. Furthermore, because the applicable regulations are no longer implemented by the Department of State, the Secretary of State is also dismissed.

IV. *Scope of Relief*

20Plaintiff requests that in addition to declaratory relief, the court issue a permanent injunction against defendants barring nationwide application of the encryption regulations on the grounds that loss of First Amendment freedoms constitutes irreparable injury, Elrod v. Burns, 427 U.S. 347, 373, 96 S.Ct. 2673, 2689–90, 49 L.Ed.2d 547 (1976), and that he will not be afforded complete relief unless an injunction extends to students, colleagues and others not before the court. ***1310** Bresgal v. Brock, 843 F.2d 1163 (9th Cir.1987). Defendants protest that a nationwide injunction is improper because relief should be no broader than necessary, *Meinhold v. United States Dept. of Defense,* 34 F.3d 1469, 1480 (9th Cir.1994), and because the issues are novel and of public importance. *Azurin v. Von Raab,* 792 F.2d 914, 915 (9th Cir.1986).

In *Bresgal,* the Ninth Circuit found in the absence of a certified nationwide class that a district court could still order nationwide relief in order to ensure the prevailing parties were given the relief to which they were entitled so long as the injunction was directed against a party to the action, in that case the Secretary of Labor. 843 F.2d at 1170–71. However, this holding must still be weighed against the rule that an injunction should be no more burdensome than necessary to afford complete relief. *Meinhold,* 34 F.3d at 1480 (quoting *Califano v. Yamasaki,* 442 U.S. 682, 702, 99 S.Ct. 2545, 2558–59, 61 L.Ed.2d 176 (1979)). In this instance the court, particularly given its determination of *facial* invalidity of the regulations, could indeed order nationwide relief. However, as it did in *Bernstein II,* the court concludes that because the legal questions at issue are novel, complex and of public importance, the injunctive relief should be as narrow as possible pending appeal. *See Azurin,* 792 F.2d at 915. While declaratory relief should be sufficient, plaintiff should not fear prosecution for teaching and writing about encryption. Nor should plaintiff have to conduct his scholarly activities under stipulation with the government. Accordingly, defendants are enjoined from

enforcing the regulations against plaintiff or against anyone who seeks to use, discuss or publish plaintiff's encryption program.

V. *Effect of Previous Order*

Defendants ask the court to vacate its order in *Bernstein II* as the controversy has shifted to the new regulations and Category XIII of the USML no longer covers plaintiff's software. Plaintiff argues the court should reaffirm its previous order because the President left open the possibility that jurisdiction would be shifted back to the Department of State if export controls under the Commerce Department prove inadequate. The likelihood of the jurisdiction being transferred back to the State Department seems too remote to justify maintaining an order that no longer applies to the controversy before the court. While the government cannot avoid the constitutional deficiencies of its regulations by rotating oversight of them from department to department, the court does not believe that such was the intent here. Moreover, should the President direct that export controls on encryption be regulated under the ITAR once more, plaintiff can come back before this court at that time. However, given the continuing validity of the rationale in *Bernstein II* to the present order, neither is it necessary to vacate that decision. Accordingly, the court's holding in *Bernstein II,* in so far as it relates to the ITAR, is hereby superseded by the present order.

CONCLUSION

For the aforementioned reasons,

1) plaintiff's motion for summary judgment is GRANTED in part and DENIED in part in accordance with the foregoing;

2) defendants' motion for summary judgment is DENIED in part and GRANTED in part in accordance with the foregoing;

3) the Departments of State, Energy, Justice and the Central Intelligence Agency are dismissed as defendants;

4) the court's holding in *Bernstein v. United States Dept. of State,* 945 F.Supp. 1279, is superseded by this order;

5) the court declares that the Export Administration Regulations, 15 C.F.R. Pt. 730 et seq.(1997) and all rules, policies and practices promulgated or pursued thereunder insofar as they apply to or require licensing for encryption and decryption software and related devices and technology are in violation of the First Amendment on the grounds of prior restraint and are, therefore, unconstitutional as discussed above, and shall not be applied to plaintiff's publishing of such items, including scientific papers, algorithms or computer programs;

6) defendants are permanently enjoined from doing or causing to be done the following acts:

***1311** a) further and future enforcement, operation or execution of the statutes, regulations, rules, policies and practices declared unconstitutional under this order, including criminal or civil prosecutions with respect to plaintiff or anyone who uses, discusses or publishes or seeks to use,

discuss or publish plaintiff's encryption program and related materials described in paragraph 5) of this order; and

b) threatening, detaining, prosecuting, discouraging or otherwise interfering with plaintiff or any other person described in paragraph 6) above in the exercise of their federal constitutional rights as declared in this order.

IT IS SO ORDERED.