Cornell International Law Journal

Volume 17
Issue 1 *Winter 1984*

Article 5

Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation

Kenneth J. Pierce

PUBLIC CRYPTOGRAPHY, ARMS EXPORT CONTROLS, AND THE FIRST AMENDMENT: A NEED FOR LEGISLATION

TABLE OF CONTENTS

INTRODUCTION

The United States Government is increasing its efforts to stem the flow of technological information from the United States to foreign nations, particularly the Soviet Union.[1] The federal government controls the international transfer of arms technology through the International Traffic in Arms Regulations (ITAR),[2] a set of export licensing procedures that includes a system of prior restraints of domestic publications.[3] This Note analyzes the constitutionality of the ITAR restraints under the first amendment[4] as applied to public cryptography[5] publications and finds that the ITAR is an unconstitutional prior restraint of public cryptography publications. The

1. *See* Abrams, *The New Effort to Control Information,* N.Y. Times, Sept. 25, 1983, § 6 (Magazine), at 22; *see generally* CONGRESSIONAL RESEARCH SERVICE REPORT TO THE HOUSE COMM. ON INTERNATIONAL RELATIONS, 95th Cong., 2d Sess., REPORT ON THE INTERNATIONAL TRANSFER OF TECHNOLOGY: AN AGENDA OF NATIONAL SECURITY ISSUES (Comm. Print 1978); REPORT OF THE PRESIDENT TO THE CONGRESS TOGETHER WITH ASSESSMENT OF THE REPORT BY THE CONGRESSIONAL RESEARCH SERVICE, INTERNATIONAL TRANSFER OF TECHNOLOGY (Comm. Print 1978) (prepared for the House Comm. on International Relations).

2. 22 C.F.R. §§ 121-30 (1983).

3. *See infra* notes 86-111 and accompanying text.

4. U.S. CONST. amend. I. cl. 2 ("Congress shall make no law . . . abridging the freedom of speech, or of the press . . . .").

5. Public cryptography is the use and development of codes by private persons, without government funds or information, for nongovernmental purposes. Cryptography is a mathematical science that transforms information into codes to prevent unauthorized persons or governments from reading the encoded information. Cryptanalysis, or code-breaking, is the related mathematical science of deciphering encoded information. Cryptology encompasses both cryptography and cryptanalysis. *See* Handelman, *Special report: Cryptographic research and the national security,* SIAM News, June 1981, at 1, col. 3 (bimonthly newspaper of the Society for Industrial and Applied Mathematics).

Note concludes by proposing to replace the ITAR with a limited system of prepublication review that would both satisfy the first amendment[6] and protect United States national security.

Section I describes the recent emergence of the public cryptography industry and the federal government's concerns with the industry's potential to harm national security. Section I also discusses various federal attempts to control the industry, including the use of the ITAR prior restraints. Section II explores the history and operation of the ITAR and explains how it restrains public cryptography publications. Section III traces the development of first amendment protections against prior restraints and describes the procedural requirements necessary for a constitutional system of restraints; it concludes that the ITAR does not provide the required procedures. Section IV discusses a national security exception to the first amendment that may operate to uphold an otherwise unconstitutional prior restraint. The section finds that the ITAR is not within the national security exception, primarily due to the ITAR's questionable congressional authorization and conflicting legislative histories. Section V provides a proposal for legislation that would authorize limited prepublication review of public cryptography research.

I

THE EMERGENCE OF A PUBLIC CRYPTOGRAPHY INDUSTRY AND FEDERAL ATTEMPTS TO CONTROL IT

Cryptology has existed as long as people have sought to shield their communications from uninvited eyes. Treatises on cryptology date back to the fourteenth century,[7] and the science has experienced exponential growth since World War II.[8] Until the last few years, only governments made extensive use of cryptology.[9] But recent progress in telecommunications and computer technologies has cre-

6. Denial of an ITAR license for a public cryptography publication and the subsequent loss of revenue to the author may constitute an unconstitutional taking of property under the fifth amendment, U.S. CONST. amend. V ("nor shall private property be taken for public use, without just compensation."), because the ITAR provides no compensation to the author. This possibly unconstitutional aspect of the ITAR is beyond the scope of this Note. *See generally The Government's Classification of Private Ideas: Hearings Before a Subcomm. of the House Comm. on Government Operations,* 96th Cong., 2d Sess. (1980) [hereinafter cited as *House Hearings*].

7. *See* Handelman, *supra* note 5, at 1, col. 4.

8. *See generally* J. BAMFORD, THE PUZZLE PALACE 338-63 (1982).

9. *See* Kahn, *The Public's Secrets,* CRYPTOLOGIA, Jan. 1981, at 20.

ated a demand for private encryption devices and techniques.[10] Consequently, a new industry, public cryptography, has emerged to meet this growing demand.[11] This industry increasingly is adorned with esoteric journals, conferences and symposia,[12] hallmarks of a promising American growth technology.

The emergence of the public cryptograpy industry is of concern to the U. S. Government. The federal government views the industry as a threat to federal security interests because of the industry's potential to expose weaknesses in the code systems used by the U. S. Government. In addition, the government fears that the industry inadvertently may alert other nations to the United States' ability to decipher their secret communications.[13]

A. PUBLIC CRYPTOGRAPHY IS A GROWTH INDUSTRY

An increasing amount of sensitive information is transmitted over and accessible through unguarded telephone wires and microwaves. "[T]he U.S. banking system alone moves some $400 billion by computer around the country every day . . . ."[14] Commercial interests and private individuals want to protect the security and confidentiality of this information.[15] Their concern with the security and privacy of electronically stored data is heightened by technological advances making electronic eavesdropping and unauthorized data manipulation relatively easy, cheap, and discreet.[16] This concern has given rise to commercial markets and research in nongovernmental encryption methods and devices.[17] Courses in cryptology

10. *See* Lipman, *Computer-Fraud Coverage Grows As Insurers Solve Policy Problems,* Wall St. J., Oct. 18, 1983, at 35, col. 4.

11. Handelman, *supra* note 5, at 4, col. 4.

12. *See id.* at 4, col. 1.

13. *See infra* notes 32-35 and accompanying text.

14. Faflick, *Opening the "Trapdoor Knapsack,"* TIME, Oct. 25, 1982, at 88.

15. Encryption methods and devices have been proposed or adopted for insurance files, medical records, and electronic fund transfer systems used by major financial institutions. *See* Buck, *Public Cryptography Study Group - A Report to the Society,* NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY, Oct. 1981, at 517. Encryption and scrambling devices are used regularly by many companies on the Fortune 500 list of America's largest corporations. *See* Kahn, *supra* note 9, at 22-23. The Federal Reserve Bank operates an underground computer system that handles the transfer of $198,000,000,000 daily between banks. The computer system is specially designed to withstand the effects of a nuclear attack. *See* Katz, *Mountain of Money,* Washington Post, Jan. 30, 1983 (Magazine), at 22.

16. It is difficult to calculate national losses from electronic theft but estimates range from $100,000,000 to $3,000,000,000 annually. These estimates include theft from electronic fund transfer systems, the U. S. Government, and credit card accounts, as well as corporate embezzlement. *See* Huntley, *Keyboard Bandits Who Want to Steal Your Money,* U.S. NEWS & WORLD REPORT, Dec. 27, 1982, at 68-69.

17. In 1978 United States exports of cryptologic devices were valued at $800,000. In 1979 they totalled $1,800,000. *See* HOUSE COMM. ON GOVERNMENT OPERATIONS, THE

are now offered at academic institutions across the country, where increasing numbers of mathematicians pursue applied and theoretical cryptology research,[18] and numerous private businesses are entering the growing public cryptography market.[19] As the number of computer terminals in American homes and offices increases, the demand to secure the confidentiality of stored information is likely to grow.

B. The National Security Agency Views the Public Cryptography Industry as a Threat to National Security

To have an effective foreign policy and adequate national security safeguards, the federal government must secure the confidentiality of sensitive communications and information. The achievement and maintenance of these goals require that the government be able to monitor the transfer of information by other governments and be able to intercept the communications of parties known to pose a threat to national interests. The federal government relies heavily on the science of cryptology for the realization of these ends.[20] The National Security Agency (NSA), the federal government's code bureau, is responsible for ensuring that federal communications and data are secure and that the government is able to intercept and to decipher foreign states' codes.[21] The NSA's duties include designing codes to protect U. S. Government information, intercepting and deciphering foreign communications, and monitoring international messages to and from the United States.[22]

The NSA grew out of the American intelligence forces of World War II[23] and is now the largest bureaucratic entity in the American intelligence community.[24] It has no legislative authorization; a still

---

Government's Classifications of Private Ideas, H.R. Rep. No. 1540, 96th Cong., 2d Sess. 72 (1980) [hereinafter cited as House Report].

18. *See* Bamford, *supra* note 8, at 350.

19. *Id.* at 340-49.

20. *See generally id.*

21. *See House Hearings, supra* note 6, at 423-26 (testimony of Adm. B.R. Inman, Director, National Security Agency). For an in-depth discussion of the NSA and its operations, see generally Bamford, *supra* note 8.

22. *See Espionage Laws and Leaks: Hearings Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence,* 96th Cong., 1st Sess. 25 (1979) (testimony of Daniel B. Silver, General Counsel, National Security Agency) [hereinafter cited as *Espionage Laws and Leaks*].

23. M. Halperin, J. Berman, R. Borosage & C. Marwick, The Lawless State 172 (1976).

24. Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Foreign and Military Intelligence, Final Report, Book 1, 94th Cong., 1st Sess. 333-34 (1975).

secret presidential memorandum established the Agency in 1952.[25] Although the NSA remains cloaked in secrecy, its cryptologic services have been of enormous value to the United States. For example, an NSA predecessor deciphered Japanese correspondences that forewarned of the bombing of Pearl Harbor.[26] Another NSA predecessor in United States Army intelligence deciphered a Japanese code during World War II that gave the United States Pacific Fleet an invaluable strategic advantage culminating in American victories in the Coral Sea and at Midway.[27] Further, the NSA first alerted the nation to Soviet efforts to install offensive missiles in Cuba in the early 1960's.[28] And in 1972, during the Strategic Arms Limitations Talks, the NSA intercepted and deciphered confidential Soviet negotiating positions. The information allowed United States diplomats to win a bilateral agreement not to build anti-ballistic missile systems.[29] It is, therefore, not surprising that Senator Walter Mondale said that he "consider[ed] . . . [the NSA] . . . to be possibly the single most important source of intelligence for this nation."[30] Indeed, history attests that when NSA methods and secrets are compromised or disclosed, potentially serious consequences to national security may result.[31]

The NSA is worried by the growth of the public cryptography industry, viewing it as a threat to the NSA's mission.[32] The Agency is concerned that a rapid growth in private cryptology research could significantly undermine its domination of the science.[33] Moreover, the private development and dissemination of algorithms used in public cryptography could alert a foreign nation, whose communica-

25. *See* HOUSE REPORT, *supra* note 17, at 63.

26. *See* BAMFORD, *supra* note 8, at 35-39. By the time the messages came through communication channels to military commanders, it was too late to prevent the catastrophe that occurred.

27. *Id.* at 43.

28. *Id.* at 215.

29. *See* Kahn, *supra* note 9, at 21 (Treaty on the Limitation of Anti-Ballistic Missle Systems, United States - Union of Soviet Socialist Republics, 23 U.S.T. 3435, T.I.A.S. No. 7503 (1972)).

30. Kahn, *supra* note 9, at 21 (quoting Sen. Walter Mondale).

31. For example, in 1960 two high level NSA cryptologists defected to the Soviet Union. A Department of Defense official is reported to have called the defection "possibly the worst security breach since Klaus Fuchs gave the Russians the secret of the atom bomb." BAMFORD, *supra* note 8, at 143. President Eisenhower labelled the pair "self-confessed traitors." Raymond, *President Calls Pair Traitorous,* N.Y. Times, Sept. 7, 1960, at 11, col. 1. President Truman concluded: "They ought to be shot . . . ." *Truman Agrees to Stump State,* N.Y. Times, Sept. 10, 1960, at 44, col. 1.

32. *House Hearings, supra* note 6, at 424 (testimony of Adm. B.R. Inman, Director, National Security Agency); *see also* Broad, *Computer Security Worries Military Experts,* N.Y. Times, Sept. 25, 1983, at 2, col. 2.

33. Address by Adm. B.R. Inman to the Armed Services Communications and Electronics Association (Mar. 1979), *The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector, reprinted in* CRYPTOLOGIA 129, 130 (July 1979).

tions the NSA now monitors and deciphers, to flaws in that nation's coding system, thereby inducing it to change its codes.[34] Finally, the NSA fears that public cryptography could threaten the security of sensitive U. S. Government information by divulging weaknesses in federal code systems or rapidly advancing other nations' abilities to decipher federal codes.[35]

C. The National Security Agency's Attempts to Control Federal Funding for and Publication of Public Cryptography Research

NSA concern with public cryptography became evident in 1975 when the Agency tried to stop all National Science Foundation (NSF) grants for cryptology research.[36] The NSA asserted that it had exclusive authority to fund cryptology research, and accordingly that NSF grants for cryptology research were illegal.[37] Although the NSF did rebuke the NSA, the two agencies subsequently have agreed on coordinated funding and review procedures under which the NSA reviews NSF cryptology research grant applications to determine whether the proposed research presents any threats to national security.[38] Thus, the NSA has acquired control of NSF

34. *Id.* at 130-32.

35. *Id.* An unspoken concern of the NSA is that private individuals and companies may develop and begin to employ codes so secure that even the NSA can not decipher them. This is allegedly one reason why the NSA became involved in the National Bureau of Standards' contract with IBM to develop an encryption system for private and government records, known as the Data Encryption Standard. "[S]ome critics suspect that this coding system was carefully designed to be just secure enough so that corporate spies outside the government could not break a user's code and just vulnerable enough so that the National Security Agency could break it." Kolata, *Computer Encryption and the National Security Connection,* SCIENCE, July 29, 1977, at 438. It is feasible that the private sector will develop unbreakable codes. "At the Massachusetts Institute of Technology, . . . [cryptologists have] . . . proposed a system employing the 'public key' approach. Known as the R.S.A. system, it is widely regarded as unbreakable, given present computer capabilities." Sullivan, *Tighter Security Rules for Advances in Cryptology,* N.Y. Times, June 1, 1981, at 17, col. 3. *But cf.* Faflick, *supra* note 14 (description of how one "public key" code was broken).

36. *See* Memorandum from F. Weingarten, National Science Foundation, to General Counsel, National Science Foundation (June 13, 1975), *reprinted in House Hearings, supra* note 6, at 762. During this same period the NSA also unsuccessfully attempted to have the United States Patent Office place secrecy orders on patent requests for encryption devices. HOUSE REPORT, *supra* note 17, at 21-24. That NSA effort may have been authorized by the Inventions Secrecy Act, 35 U.S.C. §§ 181-88 (1976 & Supp. V 1981). The possible use of the Inventions Secrecy Act to control public dissemination and marketing of cryptologic devices for which patents have been requested is beyond the scope of this Note. For a description of the Act and its possible application to public cryptography research, see HOUSE REPORT, *supra* note 17, at 161.

37. Memorandum from J. Lasken, Assistant to the General Counsel, National Science Foundation, to F. Weingarten, National Science Foundation (June 19, 1975), *reprinted in House Hearings, supra* note 6, at 763.

38. File Memorandum from F. Weingarten, National Science Foundation (May 3, 1977), *reprinted in House Hearings, supra* note 6, at 764-65; Letter from J. Pasta, National

funding of cryptology research at American academic institutions and elsewhere.

The public first became aware of the NSA's fears of privately funded cryptology research in 1977 when an NSA employee wrote a letter to the Institute of Electrical and Electronics Engineers (IEEE)[39] warning that a scheduled conference at Cornell University might violate the International Traffic in Arms Regulations (ITAR).[40] The letter advised the IEEE that the symposium's sessions on cryptography could subject participants to severe criminal sanctions if the IEEE did not acquire licenses from the State Department prior to the symposium.[41] Although the letter apparently lacked formal NSA authorization,[42] it sent a chill through the conference.[43] Since this incident, the use of the ITAR as a prepublication restraint on public cryptography has been found to be an unconstitutional prior restraint of speech in an internal, nonbinding[44] Justice Department memorandum,[45] and has been the subject of congressional hearings.[46]

Science Foundation, to C. Corry, National Security Agency (Nov. 28, 1977), *reprinted in id.* at 768; Letter from R. Atkinson, National Science Foundation, to Adm. B. R. Inman, National Security Agency (Sept. 7, 1978), *reprinted in id.* at 770-71; Letter from Adm. B.R. Inman, National Security Agency, to R. Atkinson, National Science Foundation (Sept. 21, 1978), *reprinted in id.* at 772; Letter from R. Atkinson, National Science Foundation, to Adm. B. R. Inman, National Security Agency (Dec. 27, 1978), *reprinted in id.* at 773.

39. *See House Hearings, supra* note 6, at 426-27 (statement of Rep. Richardson Preyer).

40. 22 C.F.R. §§ 121-30 (1983). For a discussion of the ITAR, see *infra* notes 86-111 and accompanying text.

41. *House Hearings, supra* note 6, at 426-27 (statement of Rep. Richardson Preyer).

42. *Id.* at 427 (testimony of Adm. B.R. Inman, Director, National Security Agency).

43. Kahn, *supra* note 9, at 24. A Stanford University graduate student was informed by Stanford's lawyers that Stanford might be unwilling to incur the legal costs which could arise from prosecution under the ITAR, as it would were a member of Stanford's faculty prosecuted. Consequently, the student's paper was presented by the student's faculty advisor. Letter from Professor Toby Berger, Cornell University, to Ken Pierce (Apr. 28, 1984) (letter on file at the offices of the Cornell International Law Journal).

44. *See House Hearings, supra* note 6, at 266-67 (testimony of H. Miles Foy, Office of Legal Counsel, Department of Justice).

45. Memorandum from J. Harmon, Department of Justice, to F. Press, Science Advisor to the President (May 11, 1978), *reprinted in House Hearings, supra* note 6, at 268-84. "[I]t is our view that the existing provisions of the ITAR are unconstitutional insofar as they establish a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector." *Id.* at 284.

46. *See generally House Hearings, supra* note 6.

D. The Public Cryptography Study Group's Voluntary System of Prepublication Review of Public Cryptography Research Has Failed

The letter to the IEEE and the public's growing awareness of NSA involvement in NSF cryptology grant proposals and private patent applications[47] drew criticism from the academic community.[48] In response to that criticism, Robert Inman, then director of the NSA, publicly outlined the Agency's concerns with public cryptography.[49] Acting on a request from Inman, the American Council on Education convened the Public Cryptography Study Group.[50] The goals of the Study Group arguably presented an insolvable dilemma. The Group was to recommend a procedure under which academic freedom to pursue public cryptography research would be protected but simultaneously would be controlled in such a way as to pose a minimal threat to the NSA's mission and national security.[51] During the Study Group's meetings the NSA made the Group aware of the Agency's position that the ITAR authorizes a prior restraint on public cryptography publications,[52] of the Justice Department's memorandum[53] questioning the constitutionality of this application of the ITAR,[54] of the NSA's desire for a uniform system of prepublication review,[55] and of the NSA's general legislative proposal to replace the ITAR.[56]

---

47. *See* HOUSE REPORT, *supra* note 17, at 21-26.

48. *See, e.g., House Hearings, supra* note 6, at 416-23 (testimony of George Davida, Associate Professor, Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee); *id.* at 406-16 (testimony of David Kahn, author and past president of the New York Cipher Society and of the American Cryptogram Association); Ferguson, *Scientific Freedom, National Security, and the First Amendment,* SCIENCE 620-24 (Aug. 12, 1983).

49. *See* Address by Adm. B.R. Inman, *supra* note 33.

50. *See* American Council on Education, *Public Cryptography Study Group—A Report to the Society,* NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY 518 (Oct. 1981) [hereinafter cited as American Council on Education].

51. *Id.* at 517-18.

52. *See* Memorandum from D. Schwartz, General Counsel, National Security Agency, to the Public Cryptography Study Group (May 6, 1980), *reprinted in House Hearings, supra* note 6, at 707. Attached to the memorandum was a copy of the Address by Adm. B.R. Inman, *supra* note 33. In the address Inman stated: "The Agency has also recognized that ambiguities in the definitional provisions of the ITAR could be viewed as inhibiting international scholarly exchanges on matters relating to cryptology. Another ambiguity in the regulation could be viewed as imposing a requirement of prior governmental review on domestic scholarly publications."

53. *See* Memorandum from J. Harmon, *supra* note 45.

54. *See* American Council on Education, *supra* note 50, at 520.

55. *See* Minutes of the Second Meeting of the Public Cryptography Study Group (May 29, 1980), *reprinted in House Hearings, supra* note 6, at 702.

56. The NSA recommended a system of restrictions based on either prepublication review, presumably by the NSA, or postpublication criminal sanctions. Either system would have applied to an undefined core of cryptologic information. The amount of information actually affected would have been quite large, as both proposals provided

The Study Group rejected both the use of the ITAR to control public cryptography research and the NSA legislative proposal.[57] It settled[58] instead on a voluntary system[59] of prior review under which the NSA could recommend changes in a monograph before publication.[60] Many cryptology researchers, however, are dissatisfied with the Study Group's proposal.[61] They believe that the proposal constitutes an infringement on academic freedom, and they are concerned by the NSA's authority under the proposal to censor their work. To date, the Study Group's proposal has been "all but officially ignored"[62] by those whom the Study Group hoped would participate.

The NSA tentatively accepted the Study Group's voluntary sys-

---

for the restraint of publications "likely to have a discernible adverse impact on the national security." Although the proposals alluded to some type of "judicial review," publication of an article on public cryptography without first obtaining a license from the NSA would be a crime under both proposals. *See* American Council on Education, *supra* note 50, at 520-21. In testimony to Congress, Inman reiterated the NSA's desire for prepublication review of public cryptography publications. *House Hearings, supra* note 6, at 427 (testimony of Adm. B.R. Inman, Director, National Security Agency).

57. American Council on Education, *supra* note 50, at 522-23.

58. The Study Group's report was not unanimous; it included a dissent against any form of government review of academic research. *See* Davida, *The Case Against Restraints on Non-governmental Research in Cryptography, reprinted in* American Council on Education, *supra* note 50, at 524-26.

59. Voluntary censorship systems have been established in the past with mixed results. During World War I the federal government established a voluntary press censorship system to control the dissemination of information detrimental to the war effort. The government asked reporters to adhere to the self-censorship regulations issued by the Departments of State, War, and Navy. The program largely was ineffective because the censored information appeared in publications other than those participating in the program. Another unsuccessful system was the Office of Strategic Information, established in 1954 by the Commerce Department, which set up a voluntary system to stop United States businessmen from sending unclassified strategic data to foreign nations. That program was not well received and largely was ineffective. In contrast, when the Office of Censorship, established in 1941, issued a narrow Code of Wartime Practices and identified types of military information which might be helpful to the enemy, voluntary compliance was generally good. *See* J. WIGGINS, FREEDOM OR SECRECY 95-104 (1956). *See also Espionage Laws and Leaks, supra* note 22, at 44-45 (testimony of Robert Keuch, Deputy Asst. Attorney General, Department of Justice) ("I know of a number of cases . . . [of government sponsored voluntary censorship systems] . . . and we have had a mixed result." *Id.* at 45).

60. American Council on Education, *supra* note 50, at 523-24.

61. *See* Davida, *supra* note 58; Burnham, *Government Restricting Flow of Information to the Public,* N.Y. Times, Nov. 15, 1982, § A, at 1, col. 4 (subcommittee of the American Association of University Professors lodged a protest against these and other governmental actions that the subcommittee viewed as serious infringements on academic freedom); Handelman, *supra* note 5, at 5, col. 1 (scientist doing cryptography research turned down a National Science Foundation grant because he feared NSA control of his funding and research).

62. BAMFORD, *supra* note 8, at 363.

tem and outlined procedures for its operation.[63] But the NSA is not bound by the Study Group's proposal. Faced with the widespread noncooperation with the voluntary system, the Agency has threatened to enforce restrictive laws that would establish an effective system of prepublication review of public cryptography research.[64] Given the past actions of the federal government and recent events,[65] these restrictive laws are most likely to be the ITAR.

II

PREPUBLICATION CONTROL OF PUBLIC CRYPTOGRAPHY RESEARCH BY ENFORCEMENT OF THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS

One goal of the National Security Agency is to establish uniform prepublication review of public cryptography research.[66] The Study Group's voluntary censorship proposal can not guarantee such review. Similarly, post publication criminal sanctions under the Espionage and Censorship Statutes,[67] which provide penalties for the intentional disclosure of classified information,[68] also fail to meet NSA concerns. While the espionage statute specifically related to the disclosure of federal cryptology systems[69] "makes prosecution easier than any of the other espionage laws,"[70] it only applies to clas-

63. Letter from L. Fauren, Director, National Security Agency, to W. LeVegue, Executive Director, American Mathematical Society (Apr. 22, 1982), *reprinted in* NOTICES OF AMERICAN MATHEMATICAL SOCIETY 322-23 (June 1982).

64. *See* BAMFORD, *supra* note 8, at 363.

65. *See supra* note 52 and accompanying text. *See also* Greenberg, *'Remote Censoring': DOD Blocks Symposium Papers,* SCIENCE NEWS 148 (Sept. 4, 1982) (Departments of State, Commerce, and Defense used threat of the ITAR sanctions to force the removal of over one hundred unclassified papers from an August 1982 international symposium on optical engineering in San Diego); Wade, *Science Meetings Catch the U.S. - Soviet Chill,* SCIENCE 1056 (Mar. 7, 1980) (threats of the ITAR sanctions used to disinvite Soviet scientists from the American Vacuum Society's February 1980 conference on bubble memory); Note, *Arms Control - State Department Regulation of Exports of Technical Data Relating to Munitions Held to Encompass General Knowledge and Experience,* 9 N.Y.U. J. INT'L L. & POL. 91, 101 (1976) (acting under the ITAR, State Department refused to issue licenses to a group of American Scientists preparing to address a conference on space technology in Madrid, thus preventing the scientists from delivering papers on rocket propulsion and reentry problems of space vehicles); *see generally* Abrams, *supra* note 1.

66. *See* Address by Adm. B.R. Inman, *supra* note 33, at 134-35; Shapley, *Intelligence Agency Chief Seeks "Dialogue" with Academics,* SCIENCE 407 (Oct. 27, 1978).

67. 18 U.S.C. §§ 791-99 (1982).

68. *See* Gorin v. United States, 312 U.S. 19 (1941) (holding that scienter is required for conviction under the Espionage and Censorship Statutes).

69. 18 U.S.C. § 798(a) (1982).

70. *Espionage Laws and Leaks, supra* note 22, at 26 (testimony of Daniel B. Silver, General Counsel, National Security Agency).

sified information and may not be invoked until after publication.[71] Unfortunately, once the key to a code is published, damage to national security is complete. Moreover, the criminal trial necessary to the statute's enforcement may expose information even more harmful to national security than the published disclosure.[72] Generally, the Executive constitutionally is constrained from placing prior restraints on private publications[73] absent congressional authorization[74] or an employment or contract relationship between the author and the federal government.[75]

To prevent potential harm to national security, the State Department placed public cryptography publications under the ITAR licensing system.[76] These regulations establish a system of prior restraint on public cryptography research.[77] They are, however, based on questionable legislative authority.[78]

---

71. 18 U.S.C. § 798(a) (1982).

72. This sometimes is referred to as the "greymail" problem. *See generally* HOUSE COMM. ON GOVERNMENT OPERATIONS, JUSTICE DEPARTMENT HANDLING OF CASES INVOLVING CLASSIFIED DATA AND CLAIMS OF NATIONAL SECURITY, H.R. REP. NO. 280, 96th Cong., 1st Sess. (1979).

73. *See infra* notes 122-29 and accompanying text. For a discussion of a judicially developed exception to this principle, the national security exception, see *infra* notes 146-65 and accompanying text.

74. For a discussion of this doctrine and the lack of congressional authorization of the ITAR, see *infra* notes 217-53 and accompanying text. Congress has authorized prior restraints by the Executive in only a few narrow instances, most notably the publication of information for the development of atomic weapons. The Atomic Energy Act places a government security classification on private atomic weapons research. 42 U.S.C. §§ 2161-66 (1976 & Supp. V 1981). This statute embodies the notion of "born classified" wherein all information of this nature is subject to a blanket prior restraint. *See generally,* HOUSE REPORT, *supra* note 17, at 132-42. Use of the Act to restrain a private publication regarding atomic weapons designs was upheld by a federal district court over a first amendment challenge. United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wisc. 1979), *appeal dismissed,* 610 F.2d 819 (7th Cir. 1979). The restraining order was lifted, at the government's request, when the case was rendered moot by public dissemination of the information by another source. HOUSE REPORT, *supra* note 17, at 145-46. The Inventions Secrecy Act, 35 U.S.C. §§ 181-88 (1976 & Supp. V 1981), allows the government to classify and take certain private inventions upon receipt of a patent application. The Act provides compensation for the applicant's loss of the use of his invention. This statute has not been challenged in court on first amendment grounds. *See supra* note 36.

75. *See, e.g.,* Snepp v. United States, 444 U.S. 507 (1980) (granting Executive request for a court order to stop publication of a book about public and unclassified activities of the Central Intelligence Agency (CIA) written by a former CIA employee, based upon contractual and employment duties of the author to his former government employer). These employment and contractual justifications for a prior restraint are inapplicable to public cryptography, which is, by definition, limited to the use and development of codes by private persons independent of the government. *See supra* note 5.

76. *See infra* notes 79-85 and accompanying text.

77. *See infra* notes 105-11 and accompanying text.

78. *See infra* notes 227-53 and accompanying text. Another statute, the Export Administration Act (EAA), 50 U.S.C. app. §§ 2401-20 (Supp. V 1981), and the regulations promulgated thereunder, 15 C.F.R. §§ 368-99 (1983), may operate as a prior restraint system similar to the ITAR. But the EAA's regulations defer control of the

A. History, Operation, and Application of the International Traffic in Arms Regulations

The commerce clause of the Constitution delegates to Congress the power to control United States exports.[79] In an exercise of this power, Congress enacted the Mutual Security Act of 1954.[80] Section 414 of the Act provided the President with broad authority[81] to control "the export of . . . arms, ammunition and implements of war, including technical data related thereto" in the interest of national security.[82] The ITAR originally was promulgated by the Department of State based upon this statutory language.[83] The Arms Export Control Act of 1976[84] subsequently replaced section 414 of the 1954 Act, and the State Department currently views it as legisla-

---

export of information and items related to cryptology to the ITAR. *See* 15 C.F.R. § 370.10(a) (1983). *See also* 50 U.S.C. § 2416(b) (Supp. V 1981). Although beyond the scope of this Note, the constitutionality of prior restraints under the EAA may be assessed according to the legal principles and doctrines discussed herein.

79. U.S. Const. art. I, § 8, cl. 3 ("The Congress shall have Power . . . To regulate Commerce with foreign Nations . . . ."). In a case involving a suit by the United States for contract damages and other relief against a private importer of seed potatoes in violation of an Executive agreement but consistent with statutory controls, the United States Court of Appeals for the Fourth Circuit held:

> [W]hile the President has certain inherent powers under the Constitution such as the power pertaining to his position as Commander in Chief of Army and Navy and the power necessary to see that the laws are faithfully executed, the power to regulate . . . foreign commerce is not among the powers incident to the Presidential office, but is expressly vested by the Constitution in the Congress.

United States v. Guy W. Capps, Inc. 204 F.2d 655, 659 (4th Cir. 1953), *aff'd on other grounds,* 348 U.S. 296 (1955). The Supreme Court did not address this separation of powers issue in its opinion. Indeed, the Court still has not ruled on the precise demarcation between presidential power to control the export of arms, arguably an inherent aspect of Executive foreign policy powers, and the express power of Congress to regulate foreign commerce. For a criticism of the *Capps* decision, see L. Henkin, Foreign Affairs and the Constitution 180-87 (1972). *But cf.* L. Tribe, American Constitutional Law 171 (1978).

80. Mutual Security Act, ch. 937, 68 Stat. 832 (1954), *repealed by* Arms Export Control Act of 1976, Pub. L. No. 94-329, § 212 (b)(1), 90 Stat. 745 (1976), codified at 22 U.S.C. § 2778 (1982).

81. The United States Court of Appeals for the Fifth Circuit held that the Act was not an unconstitutional delegation of power from the Congress to the Executive. Samora v. United States, 406 F.2d 1095 (5th Cir. 1969).

82. Mutual Security Act of 1954, ch. 937, § 414(a), 68 Stat. 832, 948 (1954), *repealed by* Arms Export Control Act of 1976, Pub. L. No. 94-329, § 212 (b)(1), 90 Stat. 745 (1976), codified at 22 U.S.C. § 2778 (1982). The House version of the bill did not contain the reference to related technical data. The conference committee accepted the Senate language. *See* Conf. Rep. No. 2637, 83d Cong., 2d Sess. § 414, *reprinted in* 1954 U.S. Code Cong. & Ad. News 3338, 3347. ("It is believed that control over technical data, although difficult to administer except when wartime censorship is in effect, is important to United States security and that those responsible for controlling the export and import of munitions should be given such authority.") *See also* Note *supra* note 65, at 96-98.

83. *See* 22 C.F.R. Part 121 (1983) (authority section).

84. Pub. L. No. 94-329, § 212 (b)(1), 90 Stat. 745 (1976), codified at 22 U.S.C. § 2778 (1982).

tive authority for the ITAR.[85]

The ITAR requires that articles designated by the President as "arms, ammunition, and implements of war"[86] be placed on the United States Munitions List and that their export be licensed by the Department of State.[87] A willful violation of this licensing system is punishable by a fine of up to $100,000, imprisonment up to two years, or both.[88] The Munitions List includes cryptographic devices,[89] as well as classified[90] and unclassified[91] technical data[92] related to cryptographic devices. The definition of "technical data" given by the Department of State is so broad, however, that it is difficult to determine what the term does not cover.[93] Technical data subject to the ITAR include:

---

85. *See* 22 C.F.R. Part 121 (1983) (authority section). *See also* Arms Export Control Act of 1976, Pub. L. No. 94-329, § 212 (b)(1), 90 Stat. 745 (1976), codified at 22 U.S.C. § 2778 (1982). ("Any reference to [section 1934 of this title] shall be deemed to be a reference to section 38 of the Arms Export Control Act [this section] and any reference to licenses issued under section 38 of the Arms Export Control Act [this section] shall be deemed to include a reference to licenses issued under section 414 of the Mutual Security Act of 1954.") The ITAR was not amended significantly when its legislative authority shifted from the 1954 Act to the 1976 Act. The 1976 Act gives the President authority to control munitions exports in the interests of "world peace and the security and foreign policy of the United States." 22 U.S.C. § 2778(a)(1) (1982). The 1976 Act substitutes "defense articles and defense services," 22 U.S.C. § 2778(a)(1) (1982), for the 1954 Act's phrase "arms, ammunition and implements of war, including technical data related thereto." 68 Stat. 848(a), ch. 937, § 414(a), *repealed by* Arms Export Control Act of 1976, Pub. L. No. 94-329, § 212 (b)(1), 90 Stat. 745 (1976), codified at 22 U.S.C. § 2778 (1982). Unfortunately, the legislative history of the 1976 Act offers no explanation why Congress did not retain the "technical data related thereto" language of the 1954 Act. H.R. REP. No. 94-1144, 94th Cong., 2d Sess. (1976), S. REP. No. 94-876, 94th Cong., 2d Sess. (1976), CONF. REP. No. 94-1272, 94th Cong., 2d Sess. (1976), *reprinted in* 1976 U.S. CODE CONG. & AD. NEWS 1378-1454. Presidential authority under the 1976 Act is delegated to the Secretary of Defense and the Secretary of State. Exec. Order No. 11,958, 3 C.F.R. § 79 (1978).

86. 22 C.F.R. § 121.01 (1983). Although the Arms Export Control Act of 1976 substituted "defense articles and defense services" for the terms "arms, ammunition and implements of war" of the Mutual Security Act of 1954, see *supra* note 85, the ITAR retains the terminology of the earlier Act.

87. 22 C.F.R. § 123.01 (1983).

88. 22 U.S.C. § 2778(c) (1982).

89. 22 C.F.R. § 121.01, Category XIII(b) (1983) ("Speech scramblers, privacy devices, cryptographic devices (encoding and decoding), and specifically designed components therefore, ancillary equipment, and especially devised protective apparatus for such devices, components, and equipment").

90. 22 C.F.R. § 121.01, Category XVII (1983).

91. 22 C.F.R. § 125.04(a) (1983).

92. 22 C.F.R. § 121.01, Category XVIII (1983).

93. *See* United States v. Edler Industries, Inc., 579 F.2d 516, 519 (9th Cir. 1978) (upholding conviction under the ITAR for the unlicensed export of missile technology to a French company over a first amendment overbreadth challenge): "The basic principles of the diesel engine, for example, constitute unclassified information that can be used in the manufacture of military trucks, which are included in category VII(d) of the U.S. Munitions List." (citing 22 C.F.R § 121.01 (1977)).

> (a) Any unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of arms, ammunition, and implements of war on the U.S. Munitions List; or
> (b) any technology which advances the state-of-the-art or establishes a new art in an area of significant military applicability in the United States.[94]

The definition of the term "export" adopted by the Department of State for purposes of the ITAR also is ambiguous. Under the ITAR an export of technical data takes place:

> whenever the information is to be exported by oral, visual, or documentary means. Therefore, an export occurs whenever technical data is, inter alia, mailed or shipped outside the United States, carried by hand outside the United States, disclosed through visits abroad by American citizens (including participation in briefings and symposia) and disclosed to foreign nationals in the United States (including plant visits and participation in briefings and symposia).[95]

The Arms Export Control Act of 1976 gives the President[96] broad discretion to control arms exports,[97] and the Department of State makes full use of this discretion in defining the applicability of the ITAR licensing system[98] and its criminal penalties.[99] The ITAR does exempt certain unclassified technical data from its licensing requirements.[100] The exemption basically is limited to information already published and widely available in the public domain.[101] This

---

94. 22 C.F.R. § 125.01 (1983).

95. 22 C.F.R. § 125.03 (1983).

96. 22 U.S.C. § 2778(a)(1) (1982). The President has delegated his authority to the Secretary of State and the Secretary of Defense. Exec. Order No. 11,958, 3 C.F.R. 79 (1978). The ITAR licensing system is administered by the Secretary of State. 22 C.F.R. § 121.21 (1983).

97. In furtherance of world peace and the security and foreign policy of the United States, the President is authorized to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services." 22 U.S.C. § 2778(a)(1) (1982).

98. The Department of State concludes that it can deny, revoke, or suspend an ITAR license without prior notice whenever it believes such action to be advisable "in furtherance of (1) World peace; (2) The security of the United States; (3) The foreign policy of the United States; or (4) Whenever the Department believes that [the Arms Export Control Act of 1976 or the ITAR has] been violated." 22 C.F.R. § 123.05 (1983).

99. 22 U.S.C. § 2778(c) (1982). *See supra* text accompanying note 88.

100. 22 C.F.R. § 125.11 (1983).

101. The ITAR exempts unclassified technical data if it:

> (1) . . . is in published form and subject to public dissemination by being:
> (i) Sold at newsstands and bookstores;
> (ii) Available by subscription or purchase without restrictions to any person or available without cost to any person;
> (iii) Granted second class mailing privileges by the U.S. Government; or
> (iv) Freely available at public libraries.

Id. See United States v. Van Hee, 531 F.2d 352 (6th Cir. 1976) (upholding conviction for conspiracy to violate the ITAR and holding that a defendant's technological expertise was a type of technical data covered by the ITAR): "The exemption obviously refers only to unclassified technical data *in published* form." *Id.* at 357 (emphasis in opinion).

exemption, however, is not self-executing; it must be applied for.[102] Upon an adverse decision by the Department of State concerning an ITAR license or an exemption, an applicant may obtain a review of his case within the Department.[103] This internal review is final and there is no requirement that the Department secure a court order before prohibiting the export of information subject to the ITAR.[104]

Public cryptography research publications are not mentioned in the Mutual Security Act of 1954 or the Arms Export Control Act of 1976 or their legislative histories.[105] But the broad, indeterminate definitions of the ITAR and the wide discretion of the Department of State thereunder bring these publications within the ITAR compass. The Department of Justice and the National Security Agency have reached this same conclusion.[106] The ITAR definitions require that the domestic publication of public cryptography research papers be licensed[107] by the Department of State if the publication is intended for export or made available to foreign nationals in the United States.[108] To obtain a license, a researcher must submit his monograph to the State Department for prior review and possible censorship.[109] Failure to seek a license before publication or publication after a license has been denied subjects a researcher to severe criminal sanctions.[110] Moreover, the Department of State need not

102. 22 C.F.R. § 125.20(a) (1983). The burden of obtaining government approval of an ITAR license or of an ITAR exemption is on the person or company seeking publication. 22 C.F.R. § 125.11(a)(1) n.3 (1983).

103. 22 C.F.R. § 123.05(c) (1983); 22 C.F.R. Part 128 (1983).

104. The ITAR licensing procedures are not subject to the rulemaking and adjudicatory provisions of the Administrative Procedures Act, 5 U.S.C. §§ 553-54 (1982). 22 C.F.R. § 128.01 (1983). However, a person whose export is subject to the ITAR possibly may initiate judicial review of a license denial *after* the export is restrained. 5 U.S.C. §§ 701-06 (1982) (judicial review). And judicial review is available for a person convicted of an ITAR violation. *See, e.g., Van Hee,* 531 F.2d 352; *Edler,* 579 F.2d 516; United States v. Donas-Botto, 363 F. Supp. 191 (E.D. Mich. 1973).

105. For the relevant legislative histories of the two acts, see H.R. REP. No. 1925, 83d Cong., 2d Sess. (1954), S. REP. No. 1799, 83d Cong., 2d Sess. (1954), CONF. REP. No. 2637, 83d Cong., 2d Sess. (1954), *reprinted in* 1954 U.S.CODE CONG. & AD. NEWS 3175-3352; H.R. REP. No. 94-1144, 94th Cong., 2d Sess. (1976), S. REP. No. 94-876, 94th Cong., 2d Sess. (1976), CONF. REP. No. 94-1272, 94th Cong., 2d Sess. (1976), *reprinted in* 1976 U.S. CODE CONG. & AD. NEWS 1378-1454.

106. *See* Memorandum from J. Harmon, *supra* note 45; *House Hearings, supra* note 6, at 253 (testimony of H. Miles Foy, Office of Legal Counsel, Department of Justice); Address by Adm. B.R. Inman, *supra* note 33, at 133.

107. Public cryptography research is unclassified technical data that can be used "in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction . . .," 22 C.F.R. § 125.01 (1983), of a cryptologic device, an item on the U.S. Munitions List. 22 C.F.R. § 121.01, Category XIII(b) (1983). Publication of public cryptography research, therefore, is subject to the ITAR licensing system.

108. 22 C.F.R. § 125.03 (1983).

109. 22 C.F.R. § 125.20(a) (1983).

110. 22 U.S.C. § 2778(c) (1982). *See supra* text accompanying note 88.

obtain a court determination before taking action under the ITAR.[111] The ITAR thus provides an Executive agency with a system of prior restraints over private publications in the science of cryptology.

III

THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS' PREPUBLICATION REVIEW OF PUBLIC CRYPTOGRAPHY RESEARCH HAS INSUFFICIENT PROCEDURAL PROTECTIONS TO BE A VALID PRIOR RESTRAINT OF SPEECH

Publications in public cryptography are a form of speech protected by the first amendment.[112] A prior restraint of protected

111. *See supra* note 104 and accompanying text.

112. Different types of speech, speech uttered under different circumstances, enjoy varying levels of constitutional protection. Traditionally, the expression of political opinions and commentary on government are most protected by the first amendment. *See* Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 838 (1978) (overturning conviction for publication of news accounts of state judiciary oversight commission). *See also infra* note 129 and accompanying text. The Court has delineated some forms of speech to which the first amendment offers only limited protection. *See, e.g.,* Brown v. Glines, 444 U.S. 348 (1979) (upholding prior restraint of soldier's petition on a military base); Greer v. Spock, 424 U.S. 828 (1975) (limiting civilian's free speech on a military base); Virginia State Board of Pharmacy v. Virginia Citizen's Consumer Council, Inc., 425 U.S. 748 (1976) (establishing lower first amendment protections for commercial speech); C.S.C. v. Letter Carriers, 413 U.S. 548 (1973) (upholding restrictions on political speech by government employees); Roth v. United States, 354 U.S. 476 (1957) (lowering first amendment protections for obscene words); Chaplinsky v. New Hampshire, 315 U.S. 568 (1942) ("fighting words" not protected by the first amendment). Although the Supreme Court never has ruled directly on the applicability of the first amendment to scientific publications like those in public cryptography, it has stated that "[t]he First Amendment protects works which, taken as a whole, have serious literary, artistic, political, or scientific value . . . ." Miller v. California, 413 U.S. 15, 34 (1973) (dictum) (upholding conviction for the mailing of unsolicited obscene materials). Publications in public cryptography are scientific endeavors that fall squarely within the parameters of the *Miller* articulation of the first amendment's scope. Moreover, because writings in public cryptography generally are of academic origin and nature, their first amendment protections are doubly ensured. *Cf.* University of California Regents v. Bakke, 438 U.S. 265, 312 (1978) ("Academic freedom, though not a specifically enumerated constitutional right, long has been viewed as a special concern of the First Amendment.") (opinion by Powell, J.); Shelton v. Tucker, 364 U.S. 479, 487 (1960) ("The vigilant protection of constitutional freedoms is no where more vital than in the community of American schools."); Sweezy v. New Hampshire, 354 U.S. 234, 250 (1956) ("The essentiality of freedom in the community of American universities is almost self-evident.") (opinion by Warren, C.J.); Dow Chemical Co. v. Allen, 672 F.2d 1262, 1275 (7th Cir. 1982) ("[W]hatever constitutional protection is afforded by the First Amendment extends as readily to the scholar in the laboratory as to the teacher in the classroom.").

The Court sometimes has employed a distinction in first amendment protections between speech and conduct. *See, e.g.,* Cox v. Louisiana, 379 U.S. 559 (1965) (Cox II). Professor Tribe says of this approach that, "[w]hile it would probably be better to bury this distinction entirely, it is likely to remain in the vocabulary of the Court and can do little harm if it is recognized that the words cannot and do not stand for a distinctive approach to the resolution of first amendment issues." L. TRIBE, *supra* note 79, at 601.

speech is not "unconstitutional *per se*."[113] Prior restraints of protected speech, however, "are the most serious and the least tolerable infringement on first amendment rights."[114] Because the ITAR licensing system is a prior restraint of publications in cryptography,[115] the ITAR's constitutionality must be assessed by referring to first amendment principles. These principles require that prior restraints provide certain procedural safeguards to be constitutional.[116] Of particular relevance[117] is the requirement of a judicial

---

The Court of Appeals for the Ninth Circuit applied a speech-conduct distinction to uphold the ITAR against a first amendment challenge. United States v. Edler Industries, Inc. 579 F.2d 516, 521 (9th Cir. 1976). Defendants were convicted for exporting missile and rocket technology to a French corporation after having been denied an ITAR license for the export. The court held that the ITAR "control[s] the conduct of assisting foreign enterprises to obtain military equipment and related technical expertise." 579 F.2d at 521. The court's attempt to segregate proscribed conduct from protected speech under the ITAR is not convincing. It fails for the same reason that undermines any use of this analytical dichotomy: all speech involves some conduct. The dichotomy offers no predictability for future cases; it amounts to no more than ad hoc rationalization. Thus *Edler* provides no clues to a structured reasoning that could lift public cryptography publications from the first amendment protections they enjoy. The Department of Justice has reached a similar conclusion: "[W]hile the Ninth Circuit's decision is helpful in resolving First Amendment issues with respect to blueprints and similar types of technical data used as a basis for producing military equipment, we do not believe that it either resolves the First Amendment issues presented by restrictions on export of cryptographic ideas or eliminates the need to reexamine the ITAR." Letter from L. Hammond, Deputy Assistant Attorney General, Department of Justice, to W. Kay, Office of Science and Technology Policy (August 29, 1978), *reprinted in House Hearings, supra* note 6, at 264-65.

113. Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 558 (1975) (invalidating prior restraint on the performance of the musical production "Hair").

114. Nebraska Press Assn. v. Stuart, 427 U.S. 539, 559 (1976) (overturning prior restraint of the press imposed to protect a criminal defendant's right to a fair trial).

115. *See supra* notes 105-11 and accompanying text.

116. *See infra* notes 130-34 and accompanying text.

117. Another first amendment principle applicable in the context of the ITAR's prior restraint of public cryptography research is the overbreadth doctrine. The due process doctrine of void-for-vagueness also is relevant. Because, however, the ITAR is constitutionally infirm for the procedural deficiency of a lack of judicial review before a prior restraint is imposed, see *infra* notes 130-37 and accompanying text, analysis of the overbreadth and void-for-vagueness objections is beyond the scope of this Note. A general, preliminary discussion of these issues, however, is appropriate.

Federal control over foreign commerce is constitutional and limitations on the export of arms fall within the permissible boundaries of this power. *See* United States v. Gurrola-Garcia, 547 F.2d 1075 (9th Cir. 1976) (affirming conviction for violation of arms export regulations over a challenge that the authorizing statute was an unconstitutional delegation of power). Nevertheless, "a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms." NAACP v. Alabama, 377 U.S. 288, 307 (1964) (holding unconstitutional Alabama's demand that the NAACP reveal the names and addresses of all its agents and members in the state). Legislation that serves a valid government interest but proscribes activities protected by the first amendment may be held unconstitutional under the overbreadth doctrine. *See generally* Note, *The First Amendment Overbreadth Doctrine,* 83 HARV. L. REV. 844 (1970). A statute that is overbroad, however, might be upheld if an authoritative judicial interpretation of the statute limits its coverage to activities that the govern-

ment constitutionally may regulate. *See, e.g.,* Cox v. New Hampshire, 312 U.S. 569 (1941) (Cox I) (upholding state statute that required a license for a "parade or procession" on a public street in light of state supreme court's interpretive narrowing of the statute's scope and application). *Cf.* Shuttlesworth v. Birmingham, 394 U.S. 147 (1969) (striking down a narrow interpretation of a parade licensing statute by a state supreme court that was issued four years after defendant was arrested for violation of the statute).

The Arms Export Control Act of 1976 and the ITAR achieve the valid governmental interest of controlling arms exports, but the prior restraints that they impose on public cryptography publications impinge on first amendment liberties and thus could subject the licensing system to an overbreadth challenge. *See* Memorandum from J. Harmon, *supra* note 45, at 283-84. In United States v. Donas-Botto, 363 F. Supp. 191 (E.D. Mich. 1973), defendants were indicted for conspiracy to export an armored car to Portugal without an ITAR license. Defendants were charged with supervising the dismantling of the vehicle in Portugal to facilitate a process known as reverse engineering. These latter acts were charged to be in violation of the ITAR as unlicensed exports of technical knowledge. Defendants made an overbreadth challenge, claiming that the application of the regulations to technical knowledge, as opposed to the export of goods, violated the first amendment. The district court denied a motion to dismiss, holding: "[A]lthough First Amendment rights are to be closely guarded, when matters of foreign policy are involved the government has the constitutional authority to prohibit individuals from divulging 'technical data' related to implements of war to foreign governments." *Id.* at 194. The court apparently found the defendants' activities not protected by the first amendment in the presence of a congressional intent to place technical knowledge within the statute's purview. In *Edler,* 579 F.2d 516, a conviction under the ITAR was reversed on evidentiary grounds and remanded for a new trial. Defendants were charged with providing information and expertise to a French missile company after their application for an ITAR license was denied. The Court of Appeals for the Ninth Circuit construed the ITAR in the light of its promulgation under the Mutual Security Act of 1954 and rejected defendants' overbreadth arguments. Recognizing the overbreadth challenge and that "an expansive interpretation of technical data relating to items on the Munitions List could seriously impede scientific research and publishing on the international scientific exchange," 579 F.2d at 519, the Ninth Circuit adopted a narrow construction of the ITAR. The court held that "[the Mutual Security Act of 1954] and the accompanying regulations prohibits [sic] only the exportation of technical data significantly and directly related to specific articles on the Munitions List . . . [and] . . . the defendant must know or have reason to know that its information is intended for the prohibited use." *Id.* at 521. Whether the Ninth Circuit's attempt to narrow the applicability of the ITAR was sufficient to preserve the regulations against the constitutional infirmity of overbreadth is beyond the scope of this Note.

The expansive scope and indeterminate nature of activities subject to the ITAR also open the regulations to a void-for-vagueness challenge. *See* Memorandum from J. Harmon, *supra* note 45, at 283-84. As noted in *Edler,* it is difficult to determine what activities do not require an ITAR license. *See supra* note 93. Hence, an arbitrary or discriminatory application of the ITAR penalties is possible. The existence of indeterminable proscribed standards of conduct and unlimited discretion in the hands of the enforcers of a statute are the crux of the void-for-vagueness doctrine. *See generally* Note, *The Void-for-Vagueness Doctrine in the Supreme Court,* 109 U. PA. L. REV. 67 (1960). Gorin v. United States, 312 U.S. 19 (1940), however, may settle any attack on the ITAR on this basis. In *Gorin*, defendants were convicted for violations of the Espionage Act of June 15, 1917. Defendants claimed that the jury instructions at their trial, which quoted from the Act's language proscribing espionage activities "related to the National defense," were unconstitutionally vague. The Court held that, in light of the Act's scienter requirement, the Act was "sufficiently specific to advise the ordinary man of its scope." 312 U.S. at 32. Because the Arms Export Control Act of 1976 also carries the requirement of a willful violation, 22 U.S.C. § 2778(c) (1982), and employs terms that closely track the statute at issue in *Gorin,* a void-for-vagueness challenge to the ITAR also should fail.

determination before a final restraint is effected.[118]

A. Development of the First Amendment Doctrine Against Prior Restraints

Governments have attempted to control publication by licensing since as early as 1501.[119] This type of prior restraint was especially prevalent in England during the sixteenth and seventeenth centuries.[120] Responding to criticism, the British common law and Parliament eventually limited the scope of licensing systems. Indeed, Blackstone noted that:

> [Freedom of the press] consists in laying no *previous* restraints upon publications, and not in freedom from censure for criminal matter when published. Every freeman has an undoubted right to lay what sentiments he pleases before the public: to forbid this, is to destroy the freedom of the press: but if he publishes what is improper, mischieviouss [sic] or illegal, he must take the consequence of his own temerity.[121]

In order to expand public support for the United States Constitution, the Framers adopted the Bill of Rights to safeguard certain freedoms.[122] First among these enumerated rights is: "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."[123] The Supreme Court has adopted a Blackstonian construction of the first amendment, under which freedom of the press is essentially freedom from prior restraints.[124] The Court has held that this construction is necessary to the liberty of the press envisioned by the Framers.[125] Indeed, in *Patterson v. Colorado,*[126] Justice Holmes wrote that the main purpose and effect of the freedom of the press clause "is to prevent all such previous restraints upon publication as had been practised by other governments

---

118. *See infra* notes 131-32 and accompanying text.

119. *See* Emerson, *The Doctrine of Prior Restraint,* 20 LAW & CONTEMP. PROBS. 648, 650 (1955).

120. *Id.*

121. 4 W. BLACKSTONE, COMMENTARIES at 151-52 (emphasis in original).

122. James Madison said when introducing the Bill of Rights in the House of Representatives: "I believe that the great mass of the people who opposed [the Constitution adopted in 1789] disliked it because it did not contain certain effectual provisions against the encroachments on particular rights . . . ." 1 ANNALS OF CONG. 433 (J. Gales ed. 1789).

123. U.S. CONST. amend. I.

124. *See* Murphy, *Near v. Minnesota in the Context of Historical Developments,* 66 MINN. L. REV. 95 (1981); *The Constitution of the United States of America: Analysis and Interpretation,* S. DOC. NO. 82, 92d Cong., 2d Sess. 936-37 (1973). The Court also has adhered to the second tenet of Blackstone's formulation: criminal sanctions may follow publication. *See generally* Blasi, *Toward a Theory of Prior Restraints: The Central Linkage,* 66 MINN. L. REV. 11 (1981).

125. Near v. Minnesota, 283 U.S. 697, 716-18 (1932) (striking down a state statute that created a prior restraint of newspaper stories of a scandalous nature).

126. 205 U.S. 454 (1907) (upholding a state supreme court contempt order following publication of an article and a cartoon).

. . . ."[127] While an important reason for the Court's view of prior restraints as antithetical to free speech is that such restraints curtail "the advancement of truth, science, morality and arts in general,"[128] the primary purpose of the Court's construction is to ensure an informed public, "the most potent of all restraints upon misgovernment."[129]

B. The International Traffic in Arms Regulations Do Not Provide the Procedural Safeguard of Mandatory Court Review

In the few cases upholding prior restraints of speech, the Court has required that the restraints be accompanied by specific and substantive procedural safeguards.[130] In *Freedman v. Maryland*[131] the Court summarized the procedural protections necessary to sustain a system of prior restraints: (1) the government must either issue a license promptly or initiate a court proceeding to restrain publication; (2) the court proceeding must be adversarial in nature and the burden of proving that the publication is unprotected must be on the government; (3) while the government can require advance submission of a publication to a licensing board, the board's determination must be prompt and can not be administered in a manner that would "lend an effect of finality" to its decision; and (4) any restraint imposed prior to a final judicial determination must be limited to the preservation of the status quo and last for the shortest time reasonably possible.[132] The Court also places on the government the burden of demonstrating the particular facts to justify a restraint.[133] Further, if a court-ordered restraint has been imposed, the government must either stay the order pending its appeal or provide immediate appellate review.[134]

---

127. *Id.* at 462 (emphasis and citations omitted).

128. Letter from Continental Congress to the Inhabitants of Quebec (October 26, 1974), 1 Journal of the Continental Congress 108, *quoted in Near,* 238 U.S. at 717.

129. Grosjean v. American Press Co., 297 U.S. 233, 250 (1936) (striking down state licensing tax on newspapers with large circulations).

130. *See* Speiser v. Randall, 357 U.S. 513, 521 (1957) ("[When assessing government restraints on speech] the procedures by which the facts of the case are adjudicated are of special importance and the validity of the restraint may turn on the safeguards which they afford."). *See also* L. Tribe, *supra* note 79, at 734-35.

131. 380 U.S. 51 (1965) (finding a film censorship statute requiring the submission of films to an administrative board before showing to be an unconstitutional prior restraint).

132. *Id.* at 58-59.

133. *Speiser,* 357 U.S. at 526 (invalidating denial of tax exemptions to persons who could not prove that they did not advocate violent overthrow of the government).

134. Nat'l Socialist Party of America v. Village of Skokie, 432 U.S. 43, 44 (1977) (per curiam) (overturning a state court's injunction of Nazi Party demonstration where the Illinois Supreme Court had refused a petition for expedited appeal of the injunction

The ITAR, a lower federal court's recent construction of the regulations,[135] and the State Department's latest interpretation of the ITAR,[136] all fail to provide procedural protections that the Supreme Court requires for a system of prior restraints on speech. Most nota-

---

order). Although *Freedman* was a film censorship case, and *Speiser* and *Nat'l Socialist Party* respectively arose in the contexts of tax litigation and an enjoined parade, their procedural protections apply to any system of prior restraints of speech protected by the first amendment. *Conrad,* 420 U.S. at 558. *See generally* Blasi, *supra* note 124.

135. A judicial construction which imposes necessary procedural safeguards on an otherwise constitutionally infirm prior restraint statute may validate the restraint. *Freedman,* 380 U.S. at 58-59. In *Edler,* 579 F.2d 516, the Court of Appeals for the Ninth Circuit dismissed a challenge to the ITAR that was based on the regulations' procedural deficiencies. The court found the challenge to be without merit because the licensee had ample opportunity to seek administrative review of the ITAR license denial under 22 C.F.R. § 123.05 (1983) and could initiate a court review of the denial, after the restraint was effected, under the Administrative Procedure Act, 5 U.S.C. § 702 (1982). The Ninth Circuit seriously misconstrued the holding of *Freedman* and its progeny. *Freedman* and its progeny clearly hold that the burden is on the government to seek and secure a court order before a final restraint is imposed. *See supra* notes 130-34 and accompanying text. The availability of administrative review, or the opportunity for court review of the final restraint after the fact and at the initiation of the person whose publication is restrained, in no way lessens the government's burden or validates an otherwise impermissible prior restraint. That the *Edler* case does not settle the procedural infirmities of the ITAR under the constitution has been recognized by a Deputy Assistant Attorney General who noted that, "while the Ninth Circuit's decision [in *Edler*] is helpful in resolving First Amendment issues with respect to blueprints and similar types of technical data used as a basis for producing military equipment, we do not believe that it either resolves the First Amendment issues presented by restrictions on export of cryptographic ideas or eliminates the need to reexamine the ITAR." Letter from L. Hammond, Department of Justice, to W. Kay, Office of Science and Technology Policy (Aug. 29, 1978), *reprinted in House Hearings, supra* note 6, at 264-65.

136. In February 1980, the Department of State issued a statement on the ITAR, Dept. of State, 80 Munitions Control Newsletter (February 1980), *reprinted in House Hearings, supra* note 6, at 262-63, in response to the court's holding in *Edler,* 579 F.2d 516. The Newsletter reads:

> *Cryptography/Technical Data*
>
> Concern has been voiced that ITAR provisions relating to the export of technical data as applied to cryptologic equipment can be so broadly interpreted as to restrict scientific exchanges of basic mathematical and engineering research data. The Office of Munitions Control wishes to clarify the application of the technical data provisions of Section 121.01, Category XVIII, of the ITAR as applied to equipment found in Categories XI(c) and XIII(b) of the Munitions List.
>
> * * * *
>
> Cryptologic technical data for which a license is required under Section 121.01, Category XVIII, is interpreted by this office with respect to information relating to Munitions List items in Categories XI(c) and XIII(b) to include only such information as is designed or intended to be used, or which reasonably could be expected to be given direct application, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of items in such categories. This interpretation includes, in addition to engineering and design data, information designed or reasonably expected to be used to make equipment more effective, such as encoding or enciphering techniques and systems, and communications or signal security techniques and guidelines, as well as other cryptographic and cryptanalytic methods and procedures. It does not include general mathematical, engineering or statistical information, not purporting to have or reasonably expected to be given direct application to equipment in such categories. It does not

bly absent is the required provision for a judicial determination before a final restraint is imposed. Thus, unless a constitutional exception applies to prior restraints of public cryptography publications, the ITAR, as noted by the Department of Justice,[137] is an unconstitutional prior restraint.

IV

A NATIONAL SECURITY EXCEPTION TO THE FREEDOM OF SPEECH FROM PRIOR RESTRAINTS DOCTRINE

Prior restraints of speech "are not unconstitutional *per se*,"[138] and first amendment protection is not "absolutely unlimited."[139] In a few special areas, legislatures have authorized and the Supreme Court has upheld prior restraints.[140] In particular, the Court has recognized a few narrow exceptions to the first amendment under which prior restraints are constitutional, even if the restraints fail to satisfy the procedural requirements of *Freedman* and its progeny.

---

include basic theoretical research data. It does, however, include algorithms and other procedures purporting to have advanced cryptologic application.

The public is reminded that professional and academic presentation and informal discussions, as well as demonstrations of equipment, constituting disclosure of cryptologic technical data to foreign nationals, are prohibited without the prior approval of this office. Approval is not required for publication of data within the United States as described in Section 125.11(a)(1). [*See supra* note 101 and accompanying text.] Footnote 3 to Section 125.11 does not establish a prepublication review requirement. [*See supra* note 102.].

The interpretation set forth in this newsletter should exclude from the licensing provisions of the ITAR most basic scientific data and other theoretical research information, except for information intended or reasonably expected to have a direct cryptologic application. Because of concerns expressed to this office that licensing procedures for proposed disclosures of cryptologic technical data contained in professional and academic papers and oral representations could cause burdensome delays in exchanges with foreign scientists, this office will expedite consideration as to the application of ITAR to such disclosures. If requested, we will, on an expedited basis provide an opinion as to whether any proposed disclosure, for other than commercial purposes, of information relevant to cryptology, would require licensing under the ITAR.

The Newsletter does not significantly amend the prior restraint system of the ITAR, nor does it institute the procedural requirements necessary to a valid system of prior restraints. A House committee criticized the Newsletter because it "clarif[ies] little while insisting that algorithms can be dangerous if they purport to have advanced cryptologic application." HOUSE REPORT, *supra* note 17, at 68.

137. *See* Memorandum from J. Harmon, *supra* note 45.

138. *Conrad,* 420 U.S. at 558.

139. *Near,* 283 U.S. at 716.

140. *See, e.g.,* 29 U.S.C. § 160(a) (1976) (National Labor Relations Board empowered to issue cease and desist orders against employers found to violate protected rights of employees); 15 U.S.C. § 45(b) (1982) (Federal Trade Commission empowered to enjoin unfair methods of competition). Such orders often restrict what may be spoken or written under certain specified circumstances. *See* NLRB v. Gissel Packing Co., 395 U.S. 575, 616-20 (1969).

These exceptions include copyrighted works[141] and some publications by government employees,[142] especially those in the military.[143] In *Near v. Minnesota*[144] the Court first alluded to another qualification to the first amendment's condemnation of prior restraints of speech, a national security exception. Any allegation that public cryptography will disclose the nation's most sensitive secrets inherently involves national security issues; thus, the applicability of a national security exception to public cryptography publications must be determined in order to assess the constitutionality of the ITAR. The ITAR licensing system, although it fails to provide sufficient procedural safeguards,[145] may fall within a national security exception and thus withstand a first amendment challenge.

A. Origin and Development of a National Security Exception to the First Amendment

The Supreme Court wrote in 1931 that "the protection even as to previous restraint is not absolutely unlimited . . . . No one would question but that a government might prevent actual obstruction of its recruiting service or the publication of the sailing dates of transports or the number and location of troops."[146] Although some members of the Court have sought to limit application of this first amendment exception to times of war,[147] and others have sought to eliminate the exception completely,[148] a majority of the Court never has adopted either view.[149] In recent years the preservation of national security has been offered as justification for various govern-

141. Westermann Co. v. Dispatch Co., 249 U.S. 100 (1919) (ordering injunctive relief for copyright violations).

142. C.S.C. v. Letter Carriers, 413 U.S. 548 (1973) (upholding restrictions on political activities by federal employees).

143. Brown v. Glines, 444 U.S. 348 (1979) (upholding regulations that created a prior restraint of petitions on a military base).

144. 283 U.S. 697, 716 (1931) (dictum).

145. *See supra* note 130-37 and accompanying text.

146. *Near,* 283 U.S. at 716. " 'When a nation is at war many things that might be said in time of peace are such a hinderance to its efforts that their utterance will not be endured so long as men fight and that no Court could regard them as protected by any constitutional right.' " *Id.* (quoting Schenck v. United States, 249 U.S. 47, 52 (1919)). It is probably because of this narrow confine that the Court rarely has explicated a national security exception to the first amendment.

147. *See, e.g.,* New York Times Co. v. United States, 403 U.S. 714, 726 (1970) (Brennan, J., concurring). ("Our cases, it is true, have indicated that there is a single, extremely narrow class of cases in which the First Amendment ban on prior judicial restraint may be overridden. Our cases have thus far indicated that such cases may arise only when the Nation is at war.").

148. *See, e.g., id.* at 714-24 (Black, J., and Douglas, J., concurring).

149. *Cf.* Haig v. Agee, 453 U.S. 280, 303 (1981) (upholding passport revocation over a first amendment challenge) ("History eloquently attests that grave problems of national security and foreign policy are by no means limited to times of formally declared war.").

mental actions.[150] In some of these instances the Court has found the preservation of national security to be a sufficiently compelling interest to overcome individual rights traditionally thought to be protected by the Constitution.[151] If these decisions portend an expanded application of a national security exception to the first amendment, then the ITAR could be judged a constitutional prior restraint.

The maintenance of national security is the most compelling interest the federal government can offer to defend its actions.[152] The Court sometimes uses the term "national security" interchangeably with the phrases "war power,"[153] "foreign policy,"[154] and "national defense."[155] The Court's most common definition of national security is expansive: a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[156] This definition encompasses the activities of federal intelligence services, including the NSA.[157]

Although the scope of federal activities that legally may be pursued in the interests of national security has not been defined with precision,[158] it is clear that these activities can have an enormous impact on individual freedoms.[159] The Court recognizes, however,

150. *See, e.g., id.*; *Brown,* 444 U.S. 348 (upholding prior restraints of petitions on a military base); Greer v. Spock, 424 U.S. 828 (1975) (upholding ban on civilian petitions on a military base); United States v. United States District Court, 407 U.S. 297 (1972) (denying warrantless domestic surveilance); *New York Times Co.,* 403 U.S. 714; United States v. Robel, 389 U.S. 258 (1967) (finding employment practices at federal defense facilities unconstitutional); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1951) (enjoining Executive order to seize domestic steel mills).

151. *See* cases cited *supra* note 150. *See generally* Martin, *National Security and the First Amendment; A Change in Perspective,* 68 A.B.A.J. 680 (1982). "It is difficult to view . . . [these] . . . cases without a sense that there is a changing judicial attitude toward the kind of national security claims that were put forward and almost summarily rejected in the Pentagon Papers case." *Id.* at 684.

152. *Agee,* 453 U.S. at 307. " 'It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.' " *Id.* (quoting with approval Aptheker v. Secretary of State, 378 U.S. 500, 509 (1964)).

153. *See, e.g., Robel,* 389 U.S. at 264.

154. *See, e.g., Agee,* 453 U.S. at 300.

155. *See, e.g., Robel,* 389 U.S. at 264.

156. *Gorin,* 312 U.S. at 28.

157. *See Agee,* 453 U.S. at 307 ("Measures to protect the secrecy of our Government's foreign intelligence plainly serve . . . [national security interests] . . . ."); Snepp v. United States, 444 U.S. 507, 526 n.17 (Stevens, J., dissenting) ("In view of the national interest in maintaining an effective intelligence service, I am not prepared to say that [a prepublication review of a government employee's manuscript] is necessarily intolerable . . . .").

158. *See generally* Note, *Developments—National Security,* 85 HARV. L. REV. 1130 (1972).

159. *See, e.g.,* Korematsu v. United States, 323 U.S. 214 (1944) (upholding forced internment of Americans of Japanese heritage to prevent possibility of espionage).

that national security "cannot be invoked as a talismanic incantation to support any exercise" of federal power.[160] No "particular exercise of foreign affairs power [is] exempt from limitations in favor of individual rights,"[161] and "even the war power does not remove constitutional limitations safeguarding individual liberties."[162]

Probably because of the stringent conditions necessary to invoke the national security exception as envisioned in *Near,*[163] the Court has not defined precisely the scope of the exception. The Court utilizes no mechanical test to determine the applicability of the exception in a particular case. Rather, the Court begins its analysis with a "heavy presumption"[164] against the restraint in issue, and requires the government to prove a justification for the restraint.[165]

In *New York Times Co. v. United States,*[166] the Court denied an injunction to restrain the publication of purloined Pentagon documents regarding American involvement in the Vietnam War.[167] The Court reached this decision over Executive assertions of a national security need to prevent disclosure[168] but, in its brief *per curiam* opinion, did not expressly address the national security exception. The opinion did reaffirm earlier statements that "[a]ny system of prior restraints of expressions comes to this Court bearing a heavy presumption against its constitutional validity . . . ."[169] The government "thus carries a heavy burden of showing justification for the imposition of such a restraint."[170] The six concurring opinions and three dissenting opinions, however, expressed a wide range of views on the proper scope of a national security exception. Justices Black and Douglas took absolutist positions, that would not allow prior restraints even in times of war.[171] Justice Brennan would limit the exception to circumstances that would "inevitably, directly and

160. *Robel,* 389 U.S. at 263.

161. HENKIN, *supra* note 79, at 253.

162. *Robel,* 389 U.S. at 264. "Implicit in the term 'national defense' is the notion of defending those values and ideals which set this nation apart. For almost two centuries, our country has taken singular pride in the democratic ideals enshrined in its Constitution, and the most cherished of those ideals have found expression in the First Amendment. It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties - the freedom of association - which makes the defense of the Nation worthwhile." *Id.* (quoting Home Bldg. & Loan Ass'n v. Blarsdell, 290 U.S. 398, 426 (1934)).

163. *See supra* note 146 and accompanying text.

164. *New York Times Co.,* 403 U.S. at 714 (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963)).

165. *Id.*

166. 403 U.S. 714 (1970) (per curiam).

167. *See id.* at 714.

168. *See id.* at 731 (White, J., concurring).

169. *Id.* at 714 (quoting *Bantam Books,* 372 U.S. at 70).

170. *Id.* (quoting Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971)).

171. *Id.* at 714 (Black, J., concurring); *id.* at 720 (Douglas, J., concurring).

immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea."[172] Justices White and Stewart took a more moderate position that would require "express and appropriately limited congressional authorization for prior restraint"[173] when "direct, immediate and irreparable damage to our Nation"[174] is shown. Justice Marshall focused on the congressional history behind the particular restraint requested by the Executive.[175] Justice Marshall's analysis was most consistent with past Court holdings reconciling individual freedoms with Executive actions taken in the interest of national security but in conflict with congressional authorizations.[176] Justice Marshall stated that because Congress expressly had denied to the Executive the type of prior restraint that the government sought, the Court did not have "the power to make law" by granting the injunction.[177]

Justices Burger and Blackmun joined in a dissent by Justice Harlan[178] that enunciated a lenient standard for the application of a national security exception. Justice Harlan would allow a prior restraint if the Executive showed that the material to be restrained touched on the President's foreign policy powers and that the decision to enjoin a publication had been made by an appropriate cabinet secretary.[179] The dissenting Justices, however, primarily were troubled by the swiftness of the Court's decision. Chief Justice Burger stated, "[t]here are no doubt . . . exceptions [other than *Near's* national security exception] which no one has [had] occasion to describe or discuss."[180] Justice Blackmun wrote that the government had a "very narrow right"[181] to restrain some publications, but would have remanded the case for further development of the record.[182]

In all, seven justices wrote that a prior restraint of the press is not a per se violation of the first amendment.[183] For a time, it appeared that the test enunciated by Justice Stewart might prevail; Justice Brennan adopted it in his concurrence in *Nebraska Press*

172. *Id.* at 726-27 (Brennan, J., concurring).
173. *Id.* at 731 (White, J., concurring).
174. *Id.*
175. *See id.* at 740-49 (Marshall, J., concurring).
176. *See infra* note 225-53 and accompanying text.
177. *New York Times Co.,* 403 U.S. at 741 (Marshall, J., concurring).
178. *Id.* at 752-59 (Harlan, J., dissenting).
179. *Id.*
180. *Id.* at 749 (Burger, C.J., dissenting).
181. *Id.* at 761 (Blackmun, J., dissenting).
182. *Id.*
183. *See id.* at 724-62 (concurrences by Brennan, J., Stewart, J., White, J., Marshall, J.; dissents by Burger, C.J., Harlan, J., Blackmun, J.).

Association v. Stuart.[184] It is now clear, however, that no one test, and certainly none presenting as "formidable"[185] an obstacle to prior restraints as that proposed by Justice Stewart, ever has controlled a majority of the Court. Instead, the Court, when considering first amendment cases involving national security, appears to weigh six critical factors. These dominant concerns are: (1) the type of individual liberty infringed; (2) the magnitude of the danger to be avoided; (3) the scope of the President's power in the affected area; (4) congressional approval of the restraints; (5) whether government employees or funds are involved; and (6) whether the speech discloses classified information. It is the interplay of these factors that determines if particular speech is protected or constitutionally may be restrained to protect national security. The balance struck by weighing these interests determines whether a national security exception will apply in an individual case. There is no blanket verbalization of when the exception applies, no standard test. But when these factors have appeared in a proper combination, the Court has upheld restraints on first amendment liberties upon finding only a "substantial likelihood of serious damage to national security or foreign policy . . . ."[186] Thus, the Court has come a long way from the implied message of *Near*, that speech could be restrained under a national security justification only in times of war.[187]

By balancing these six factors it is possible to assess the constitutional validity of the ITAR's prior restraints on public cryptography publications *vis-a-vis* a national security exception. Although these publications are a protected form of speech,[188] the disclosure of federal codes and cryptologic abilities, even if disclosure is inadvertant,

184. 427 U.S. at 593 (Brennan, J., concurring).

185. *Id.* at 594.

186. *Agee,* 453 U.S. at 147. *Agee* involved the activities of a former government employee. This fact was critical to the Court's lowering of the first amendment protections of Agee's liberties. Employees of the government do have first amendments rights. *See, e.g.,* Pickering v. Board of Education, 391 U.S. 563 (1968) (reinstating a teacher who was dismissed for writing a letter criticizing a school board's handling of financial matters). But these rights may be curtailed by the government to meet important government interests. *See, e.g.,* C.S.C. v. Letter Carriers, 413 U.S. 548 (1973). This is especially true in cases involving the "specialized society" of the military. *See, e.g., Brown,* 444 U.S. at 354. In the military setting, for example, the Court has construed narrowly legislation intended to protect a soldier's first amendment rights in order to uphold the constitutionality of military regulations that banned petitions on base. *See id.* If the *Agee* test is limited to government employees, then a more protective standard would apply to private researchers. When an individual accepts government employment, information, or funding, however, he should be aware that such governmental contacts may furnish a sufficient premise for a subsequent narrowing of his first amendment liberties. *See, e.g., Snepp,* 444 U.S. 507.

187. *See supra* note 146 and accompanying text.

188. *See supra* note 112.

could cause serious damage to national security.[189] Still, these publications' potential to harm national security can not automatically place all such writings within a national security exception. The magnitude of the danger posed to national security will turn on the facts of a particular case; thus, it becomes necessary to consider each restraint individually.[190] And two other factors—whether classified information is involved and whether government employees are involved—are by definition inapplicable to public cryptography.[191] It is critical, then, to examine the remaining two factors to determine the applicability of a national security exception to the imposition of prior restraints on public cryptography publications: the scope of the relevant foreign policy powers of the President and the legislative history of the restraints. The President's foreign policy powers are involved because the government uses codes to protect its international relationships.[192] It is necessary to consider congressional history because of Congress' constitutional power to control foreign commerce[193] and because the prior restraints of the ITAR are premised on the Arms Export Control Act of 1976.[194] Weighing these factors will allow a determination of the constitutionality of the ITAR restraints.

B. Judicial Deference to Executive National Security Powers

The powers of the President to protect national security from foreign threats are vast.[195] Article II of the Constitution describes some of the Executive's powers in matters of national security.[196] The structure "of the federal government, the facts of national life,

189. *See supra* notes 32-35 and accompanying text.

190. *See* Speiser v. Randall, 357 U.S. 513, 521 (1957) ("[T]he validity of a restraint on speech in each case depends on careful analysis of the particular circumstances.").

191. *See supra* note 5.

192. *See supra* notes 32-35 and accompanying text.

193. *See supra* note 79 and accompanying text.

194. *See supra* notes 79-85 and accompanying text.

195. Judicial reluctance to impose limits on these powers is often founded in the separation of powers doctrine. Pursuant to this doctrine, the Court sometimes has taken the extreme position that matters related "to the conduct of foreign relations . . . are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference." Harisiades v. Shaughnessy, 342 U.S. 580, 589 (1952) (upholding deportation of alien on the basis of his political beliefs). *See also* Chicago & Southern Airlines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) ("Such decisions are wholly confided by our Constitution to the political departments of government, Executive and Legislative."). Even the President, when exercising his foreign policy powers, however, must not violate the first amendment. *See infra* notes 213-16 and accompanying text.

196. *See, e.g.,* U.S. CONST. art. II, § 2, cl. 1: "The President shall be Commander in Chief of the Army and Navy of the United States;" *id.* at cl. 2: "He shall have Power . . . to make Treaties . . . and . . . appoint Ambassadors."

the realities and exigencies of international relations, [and] the practices of diplomacy," however, have required a greatly expanded recognition of these Executive powers.[197] Consequently, the Supreme Court, using a separation of powers rationale, has expanded the scope of the Executive's foreign policy power beyond the language of the Constitution,[198] and accords great deference to exercises of the power.[199] This deference is greatest concerning Executive actions taken at the international level;[200] the Court is less willing to extend deference to domestic Executive actions taken for foreign policy or national security reasons.[201] In *United States v. Curtiss-Wright Corp.*,[202] the Court characterized the Executive's foreign policy power as "the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations . . . ."[203] The activities of the NSA fall within this presidential authority. Indeed, the Court said in *Haig v. Agee*[204] that "[m]easures to protect the secrecy of our Government's foreign intelligence operations plainly serve . . . [national security] interests."[205]

Judicial deference to Executive actions aimed at safeguarding national security sometimes stems from the Court's perception that the judiciary has inadequate expertise in matters of foreign policy. This consideration was important to the Court's holding in *Curtiss-Wright*.[206] The Court enunciated this view in *Chicago & Southern Airlines v. Waterman S.S. Corp.*:[207]

> The President both as Commander-in-Chief and as the nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret.[208]

---

197. HENKIN, *supra* note 79, at 37.

198. *See generally id.*, ch. II.

199. *See, e.g., Agee,* 453 U.S. at 292. "[M]atters relating to the conduct of foreign relations . . . are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference." *Id.* (quoting *Harisiades,* 342 U.S. at 589).

200. *See* L. TRIBE, *supra* note 79, at 158-63. *See also supra* note 195.

201. *See, e.g.,* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 635 (1952) (granting an injunction to enjoin President Truman's seizure of domestic steel mills during the Korean War). *See also* L. TRIBE, *supra* note 79, at 181-84; *Curtiss-Wright,* 299 U.S. at 320; *infra* note 218.

202. 299 U.S. 304 (1936) (upholding Executive embargo on the sale of arms in the Chaco region of South America).

203. *Id.* at 320.

204. 453 U.S. 280 (1981). *See supra* note 157.

205. *Id.* at 307.

206. *See id.* at 319.

207. 333 U.S. 103 (1948) (upholding Civil Aeronautics Board's award of international air routes because they ultimately were subject to Executive approval).

208. *Id.* at 111.

The Court has continued to utilize the rationale of judicial inexpertise in foreign policy matters in recent cases upholding Executive national security actions.[209] Although these recent cases involved former government employees,[210] the disposition of the Court to defer to the Executive on questions of national security could surface in a case involving a prior restraint of a public cryptography publication. For reasons discussed below,[211] a perception of judicial incompetency alone would be insufficient justification for placing public cryptography wholly outside first amendment protections. The perception, however, could lessen the government's burden to prove harm to national security before imposing a restraint on these publications.[212] In such a case the government could argue that an understanding of the mathematical intricacies of cryptology, and determination of the potential effect of a particular publication on national security, are beyond judicial competence. This could be a

209. For example, in *Snepp,* 444 U.S. 507, the Court created a constructive trust for the benefit of the government from the profits the defendant, a former employee of the CIA, earned from his book about American intelligence operations. The book contained no classified information. 444 U.S. at 511. The Court ordered the relief because the defendant had violated his contract agreement to submit his manuscript to the CIA for prepublication censorship. By basing its holding on contract and agency principles and by employing a constructive trust remedy, the Court did away with any need for the government to prove specific harm to national security. The government would have had to prove such harm had the Court affirmed the Court of Appeals for the Fourth Circuit's award of punitive damages. *See* United States v. Snepp, 595 F.2d 926 (4th Cir. 1974). The Court noted that "[p]roof of the tortious conduct necessary to sustain an award of punitive damages might force the government to disclose some of the very confidences [it wants to protect]." 444 U.S. at 514. Rather, the Court primarily relied on the general testimony of Admiral Stansfield Turner, then Director of the CIA, to support its assumption that the defendant's book posed a threat to national security. *See id.* at 512-13.

This same perception of judicial incompetence surfaced in *Agee,* 453 U.S. 280. The Court held for the government without requiring proof of what dangerous information was possessed by Agee or how it could harm national security. *See* 453 U.S. at 320 n.10 (Brennan, J., concurring). Important to the Court's holding was that Agee, like Snepp, was a former government employee and the information restrained was received by him while in the government's employment. *See supra* note 186.

Because public cryptography by definition operates without government funds or information, *supra* note 5, the judicial deference to Executive allegations of harm to national security in *Snepp* and *Agee* should not apply in a court's review of the constitutionality of the ITAR prior restraints on public cryptography publications. In cases where the government seeks to restrain purely private speech, as in public cryptography under the ITAR, the Court requires an assessment of the particular danger to national security from a specific publication before authorizing its restraint. *See Speiser,* 357 U.S. at 521.

210. *See supra* notes 186 and 209.

211. *See infra* notes 213-16 and 222-26 and accompanying text.

212. *Cf.* Hayden v. Nat'l Security Agency, 608 F.2d 1381, 1385 (D.C. Cir. 1979) (affirming denial of request under the Freedom of Information Act for NSA files) ("Especially concerning the NSA signals intelligence mission, a court cannot demand as complete a public record as in many other contexts—even other intelligence contexts—without imperiling legitimate secrecy interests.").

persuasive argument to decrease the government's burden to convince a court that a particular publication should be restrained.

The Court's deference to the President's national security powers is not unlimited, especially when domestic application of those powers is in question.[213] "[I]t is error to suppose that every case or controversy which touches foreign relations lies beyond judicial cognizance."[214] When an individual's constitutional rights are in issue, judicial deference is not an acceptable mode of review. Indeed, "[t]he Supreme Court has never invoked the political question doctrine to dismiss an individual's claim that a foreign relations action deprived him of constitutional rights."[215] Because the ITAR affects first amendment liberties, a court should not dismiss a challenge to the ITAR restraints on public cryptography solely because they involve elements of national security. The national security power, "like every other governmental power, must be exercised in subordination to the applicable provisions of the Constitution,"[216] including the first amendment.

C. The Role of Congressional Authority: Limits to Judicial Deference to Executive National Security Actions

The Executive can not place the ITAR restraints within an exception to first amendment protections simply by advancing a national security interest. But the potential applicability of a national security exception requires further analysis. It is necessary to consider congressional attitudes toward the ITAR licensing system, because the Court accords Executive national security actions greater deference when they have been authorized by statute.[217] Congressional authorization strengthens the President's hand, notwithstanding the breadth of the legislation found by the Court to contemplate the challenged action.[218] The Court takes this approach

213. *See Youngstown,* 343 U.S. 579.

214. Baker v. Carr, 369 U.S. 186, 211 (1962).

215. Henkin, *supra* note 79, at 486 n.6.

216. *Curtiss-Wright,* 299 U.S. at 320.

217. *See, e.g., Youngstown,* 343 U.S. at 635 (Jackson, J., concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate . . . ."); Dames & Moore v. Regan, 453 U.S. 654, 674 (1980) (upholding presidential transfer of all Iranian property subject to the jurisdiction of the United States: "Because the President's action . . . was taken pursuant to specific congressional authorization, it is 'supported by the strongest of presumptions and the widest latitude of judicial interpretation' . . ." (quoting *Youngstown,* 343 U.S. at 637) (Jackson, J., concurring)). *See also supra* note 74 and accompanying text.

218. *See, e.g., Dames & Moore,* 453 U.S. at 678. "[T]he enactment of legislation closely related to the question of the President's authority in a particular case which evinces legislative intent to accord the President broad discretion may be considered to

"because of the changeable and explosive nature of contemporary international relations, and the fact that the Executive is immediately privy to information which cannot be swiftly presented to, evaluated by, and acted upon by the legislature. Congress—in giving the Executive authority over matters in foreign affairs—must of necessity paint with a brush broader than it customarily wields in domestic areas."[219] Even legislative silence can evince congressional approval in the areas of national security and foreign relations,[220] provided that Congress is aware of the Executive's action.[221] Thus, if Congress authorized the ITAR prior restraints on public cryptography publications, a court would be more likely to find that the restraints are within a national security exception to the first amendment and, therefore, more likely to find them constitutionally valid.

The ITAR's prior restraints on public cryptography publications involve Executive national security powers,[222] Congress' power to control foreign commerce,[223] and a first amendment liberty.[224] The decisions of the Supreme Court call for a sophisticated analysis to balance these competing and conflicting constitutional interests. The Court determines the appropriate balance by employing an analytical model which weighs whether Congress authorized or approved of the Executive's actions, and whether the Executive and Congress possess concurrent powers in the particular area. The outcome of this analysis should determine whether the ITAR prior restraints on public cryptography fall within a national security exception to the first amendment. Justice Jackson described this analytical model in his concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*:[225]

> 1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. [Such executive actions] . . . would be supported by the strongest of presump-

'invite' measures on independent Presidential responsibility." *Id.* (quoting *Youngstown,* 343 U.S. at 637 (Jackson, J., concurring)); *Curtiss-Wright,* 299 U.S. at 320 ("[C]ongressional legislation which is to be made effective . . . within the international field must often accord to the President a degree of discretion and freedom from statutory restriction which would not be admissible were domestic affairs alone involved.").

219. *Agee,* 453 U.S. at 292 (quoting Zemel v. Rusk, 381 U.S. 1, 17 (1964)).

220. *See, e.g., id.* at 291 ("[I]n the areas of foreign policy and national security, . . . Congressional silence is not to be equated with Congressional disapproval."); *Dames & Moore,* 453 U.S. at 678; Zemel v. Rusk, 381 U.S. 1, 8-12 (1964).

221. *Dames & Moore,* 453 U.S. at 686: "a systematic, unbroken executive practice, long pursued to the knowledge of the Congress and never before questioned . . . may be treated as a gloss on 'Executive Power' vested in the President . . . ." (quoting *Youngstown,* 343 U.S. at 610-11) (Frankfurter, J., concurring)). *See Zemel,* 381 U.S. at 11.

222. *See supra* note 192 and accompanying text.

223. *See supra* note 79 and accompanying text.

224. *See supra* note 112.

225. 343 U.S. at 635 (Jackson, J., concurring).

> tions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.
> 2. When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or acquiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law.
> 3. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject.[226]

The ITAR falls within Justice Jackson's second category, the "twilight" of concurrent jurisdiction. The regulation of foreign commerce is an express constitutional power of Congress.[227] At the same time, the President's duty to protect national security encompasses the security of federal codes and the maintenance of the effective operation of the NSA.[228] Accordingly, congressional attitudes toward and actions affecting the prior restraint system of the ITAR are critical to a determination of the constitutionality of the ITAR licensing system.

The ITAR has been in existence since the enactment of the Mutual Security Act of 1954.[229] But neither the 1954 Act and the 1976 Arms Export Control Act,[230] nor their legislative histories,[231] mention the restraints imposed by the ITAR. The 1976 Act contains only general language that "the President is authorized to control the import and the export of defense articles and defense services . . ."[232] that he has designated as items on the United States Munitions List. Although the Department of State bases the ITAR prior

226. *Id.* at 635-38 (Jackson, J., concurring). The Court recently employed this model in *Dames & Moore,* 453 U.S. 654. Its application also was crucial to the concurrence of Justice White, joined by Justice Stewart, in *New York Times*: "At least in the absence of legislation by Congress, based on its own investigations and findings, I am quite unable to agree that the inherent powers of the Executive and the courts reach so far as to authorize remedies having such sweeping potential for inhibiting publications by the press." 403 U.S. at 782 (White, J., joined by Stewart, J., concurring). Justice Marshall also used the model in his concurrence: "When the Congress specifically declines to make conduct unlawful it is not for this Court to redecide those issues—to overrule Congress." *Id.* at 745-46 (Marshall, J., concurring).

227. *See supra* note 79.

228. *See supra* note 157.

229. *See supra* notes 79-85 and accompanying text.

230. *See supra* notes 84-85 and accompanying text.

231. *See supra* note 105.

232. 22 U.S.C. § 2778(a)(1) (1982).

restraints on this statutory language,[233] the language is too general to allow one to find congressional deliberation on and approval of the ITAR prior restraints on public cryptography. The Court has relied on similarly broad language in the foreign policy arena to find that Congress has "implicitly approved" a challenged Executive foreign policy action, but only when that language has been supported by other consistent congressional enactments and legislative histories.[234] The requisite consistent congressional actions are not present in this instance.[235]

The absence of congressional action limiting the licensing system's prior restraints on public cryptography during the ITAR's thirty year existence could be interpreted as constituting implicit congressional acquiesence in the restraints. But congressional approval can not be implied from legislative silence unless Congress had knowledge of the Executive action in issue.[236] Significantly, there is no evidence that Congress knew of the ITAR's prior restraints on public cryptography until Congress held hearings on the subject in 1980.[237] Even the Justice Department apparently was unaware of the restraints until 1978.[238] Since learning of the ITAR prior restraints on public cryptography, the House Committee on Government Operations has issued a report recommending that the Department of State "review and rewrite the ITAR to satisfy constitutional objections."[239] The Executive would be hard-pressed to argue that Congress, once aware of the ITAR prior restraints on public cryptography, gave implicit approval to the licensing system and acquiesced in the ITAR's abridgement of first amendment freedoms.

The Executive's power to enforce the ITAR as a prior restraint actually is "at its lowest ebb,"[240] because that action is incompatible with the expressed will of Congress. Congress, on at least two occasions, has rejected legislation that would have given the Executive prior restraint powers similar to those that the Department of State has promulgated under the ITAR. During a 1917 debate over the

233. *See supra* notes 80-85 and accompanying text.
234. *See Dames & Moore,* 453 U.S. at 680-81; *Zemel,* 381 U.S. at 8-12.
235. *See infra* notes 240-53 and accompanying text.
236. *See Dames & Moore,* 453 U.S. at 680-81; *Zemel,* 381 U.S. at 8-12.
237. *House Hearings, supra* note 6. *See generally* HOUSE REPORT, *supra* note 17, at 62-119.
238. The Department learned of the restraints from an internal memorandum. *See* Memorandum from J. Harmon, *supra* note 45. *See also House Hearings, supra* note 6, at 266-67 (testimony of H. Miles Foy, Office of Legal Counsel, Department of Justice).
239. HOUSE REPORT, *supra* note 17, at 119.
240. *Youngstown,* 343 U.S. at 668 (Jackson, J., concurring). This phrase is taken from the third stage of Justice Jackson's analytical model. *See supra* text accompanying note 226.

original Espionage Act, Congress rejected an amendment that would have given the President broad powers of prior restraint in times of national emergency. That amendment provided:

> During any national emergency resulting from a war to which the United States is a party, or from threat of such a war, the President may, by proclamation, . . . prohibit the publishing or communicating of, or the attempting to publish or communicate any information relating to the national defense which, in his judgment, is of such a character that it is or might be useful to the enemy. Whoever violates any such prohibition shall be punished by a fine of not more than $10,000 or by imprisonment for not more than 10 years, or both: *Provided,* That nothing in this section shall be construed to limit or restrict any discussion, comment or criticism of the acts or policies of the Government or its representatives or the publication of the same.[241]

Wary of this proposal's implications for first amendment freedoms, Congress rejected it and substituted in its place provisions for post-publication criminal sanctions,[242] including penalties for the disclosure of federal cryptology secrets.[243] Justice Marshall, in his concurrence in *New York Times Co.,*[244] discussed Congress' rejection of a more recent legislative proposal that also was similar to the ITAR:

> In 1957 the United States Commission on Government Security found that "[a]irplane journals, scientific periodicals, and even the daily newspaper have featured articles containing information and other data which should have been deleted in whole or part for security reasons." In response to this problem the Commission proposed that "Congress enact legislation making it a crime for any person willfully to disclose without proper authorization, for any purpose whatever, information classified 'secret' or 'top secret,' knowing, or having reasonable grounds to believe, such information to be so classified."[245]

Because Congress twice considered and twice rejected prior restraint systems like the ITAR, the constitutional validity of the ITAR licensing scheme is very doubtful. Similar reasoning led five members of the Court to reject the government's request for a prior restraint order in *New York Times Co.* To varying degrees, Justices Black,[246] Douglas,[247] Marshall,[248] White and Stewart[249] concluded that either because no statute authorized the restraint sought by the Executive or because Congress considered the matter and decided not to give the power to the Executive, such restraints were impermissible under the Constitution.

---

241. 55 CONG. REC. 1763 (1917).
242. These are in essence the present day Espionage and Censorship Statutes, 18 U.S.C. §§ 791-99 (1982).
243. *See* 18 U.S.C. § 798 (1982).
244. *See supra* notes 175-77 and accompanying text.
245. 403 U.S. at 747 (Marshall, J., concurring).
246. *Id.* at 718 (Black, J., concurring).
247. *Id.* at 720-24 (Douglas, J., concurring).
248. *Id.* at 746-48 (Marshall, J., concurring).
249. *Id.* at 732 (White, J., concurring).

Prior restraints on public cryptography are not authorized by the Arms Export Control Act of 1976, and Congress specifically has denied such powers to the President. Therefore, under the analysis enunciated by Justice Jackson in *Youngstown,*[250] which was applied by several members of the Court in *New York Times,*[251] and adopted by a majority of the Court in *Dames & Moore v. Regan,*[252] the ITAR is not within a national security exception to first amendment protection against prior restraints. The ITAR is thus an unconstitutional infringement on first amendment freedoms because of its failure to provide the procedural safeguards necessary to sustain a prior restraint.[253]

V

A LEGISLATIVE PROPOSAL FOR LIMITED PREPUBLICATION REVIEW OF PUBLIC CRYPTOGRAPHY RESEARCH

The widespread use of computers and telecommunications technology has created an expanding public cryptography industry[254] that poses an increasing threat to the protection of government cryptology secrets.[255] The prior restraints placed on this industry's publications by the ITAR licensing system operate in violation of the first amendment because of procedural deficiencies,[256] and do not fall within a national security exception.[257] The Public Cryptography Study Group's[258] voluntary system of prepublication review was unsuccessful.[259] And criminal sanctions after publication can not meet national security concerns over publications in public cryptography.[260] Prepublication review of public cryptography research may provide the only means to effectively meet the government's national security concerns.

Publications in public cryptography are a scientific endeavor that deserve first amendment protections.[261] But the competing considerations of national security and judicial competence auger for a

250. *See supra* text accompanying note 226.
251. *See supra* notes 246-49 and accompanying text.
252. 453 U.S. at 661 ("Justice Jackson in his concurring opinion in *Youngstown* . . . brings together as much combination of analysis and common sense as there is in this area . . . .").
253. *See supra* notes 130-37 and accompanying text.
254. *See supra* notes 10-12 and accompanying text.
255. *See supra* notes 32-35 and accompanying text.
256. *See supra* notes 130-37 and accompanying text.
257. *See supra* notes 226-53 and accompanying text.
258. *See supra* notes 47-51 and accompanying text.
259. *See supra* notes 47-65 and accompanying text.
260. *See supra* notes 67-72 and accompanying text.
261. *See supra* note 112.

tailoring of those protections to the specific problems posed by these publications. The ideas expressed in public cryptography publications may not possess the same need for spontaneous expression that ideas about political, economic, or social issues require.[262] A short delay in the publication of public cryptography articles may not diminish their significance and scientific value. Although the removal of portions of an article posing a threat to national security could infringe upon individual liberties, a deletion might be constitutionally justified when proven necessary to protect America's vital interests. Given public cryptography publications' potential for endangering the nation's safety,[263] the history of judicial deference in the national security area,[264] and the complex nature of this unique form of speech, limited prior restraints of public cryptography may be constitutional.

Detailed legislation from Congress authorizing a system of prior restraints on public cryptography is essential to the constitutionality of such restraints. With this legislative authority, the President's power to restrain publications that threaten national security would be "at its maximum."[265] Whether such legislation would bring the restraints wholly within a national security exception and thus completely outside of first amendment protections is unclear, however, because the parameters of the exception remain unsettled.[266] Assuming that a complete national security exception is not automatically created by congressional approval of Executive restraints, then the legislation should satisfy the procedural requirements of *Freedman* and its progeny[267] to adequately protect first amendment freedoms and to ensure the validity of the restraints.

"[A]n act touching on First Amendment rights must be narrowly drawn so that the precise evil is exposed."[268] Any legislated prior restraint of public cryptography publications should, therefore, delineate precisely the type of information to which the Congress

262. *See supra* notes 112 and 128 and accompanying text.

263. *See supra* notes 32-35 and accompanying text.

264. *See supra* notes 195-210 and accompanying text.

265. *Youngstown,* 343 U.S. at 638. (Jackson, J., concurring).

266. *See generally* Note, *supra* note 158. Although the issue of whether legislation is sufficient to invoke a national security exception is unclear, what is clear is that the exception will not operate to uphold domestic restraints in the interest of national security without congressional authorization. *See supra* notes 217-21 and accompanying text.

267. *See supra* notes 131-34 and accompanying text.

268. Schneider v. State, 390 U.S. 17, 24 (1968) (invalidating leafletting ban on first amendment grounds). "It has become axiomatic that precision of regulation must be the touchstone in an area so closely touching our most cherished freedoms." *Robel,* 389 U.S. at 265 (quoting NAACP v. Button, 371 U.S. 415, 438 (1963)).

intends that it apply.[269] To satisfy procedural requirements, the legislation must provide that either prompt publication will be allowed, or a court proceeding to restrain publication must be initiated in a timely manner.[270]

Court proceedings must be adversarial in nature[271] and must place upon the government the burden of proving that the publication should be restrained.[272] The government's burden should be to prove by clear and convincing evidence[273] the particular facts needed to justify the restraint;[274] specifically, that the publication in issue would cause serious, direct, immediate and irreparable harm to vital national security interests.[275] The legislation must provide that only a judicial determination will lead to the imposition of a final restraint,[276] and that any temporary restraint issued while a court order is sought must be for the shortest time possible.[277] If a court imposes a final restraint, the legislation must require the government

269. This definition may be difficult to delineate precisely without itself revealing national security secrets. A somewhat less precise definition may be acceptable to the Court due to the presence of national security issues, and a requirement that the government must prove particular harm to the nation from a particular publication. *See infra* notes 273-75 and accompanying text. Private and government cryptologists should aid Congress in arriving at a suitable definition.

270. *See Freedman,* 380 U.S. at 58-59.

271. *Id. See supra* notes 130-34 and accompanying text.

272. *Id.*

273. This is a stricter standard than the preponderance of the evidence standard usually employed in civil cases. The clear and convincing standard is applied in certain civil cases where judicial caution is deemed appropriate. Such cases include those involving fraud, a parol gift, the establishment of the existence and contents of a lost deed or will, and the proof of mutual mistake to justify reformation of an instrument. 9 J. WIGMORE, EVIDENCE § 2498 (Chadbourn Rev. 1981). Because this system of prior restraints will touch on first amendment liberties, judicial caution is warranted; thus the higher burden of proof is appropriate.

The Court's perception of a lack of judicial competence to discern whether a particular cryptography publication actually threatens national security might allow the federal government to abridge first amendment rights when national security would not require the prior restraint of a publication. This perception could result in judicial deference that would make the government's burden lighter than it should be. This problem could be overcome by establishing a special court comprised of judges with the necessary expertise, or staffed with specially trained clerks, to make such determinations. Finally, security procedures could be instituted to ensure that no national secrets are exposed during the course of judicial proceedings. A similar special court was created for the operation of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11 (Supp. V 1981). That court issues warrants for electronic foreign intelligence surveillance by the NSA and other federal intelligence agencies. *See generally* Note, *The Foreign Intelligence Surveillance Act: Legislating a Judicial Role in National Security Surveillance,* 78 MICH. L. REV. 1116 (1980).

274. *See Speiser,* 357 U.S. at 526. *See also supra* note 133 and accompanying text.

275. This proposal partially adopts the middle level standard advocated by Justices Stewart and White in *New York Times Co.,* 403 U.S. at 730 (Stewart, J., joined by White, J., concurring). *See supra* notes 173-74 and accompanying text.

276. *See Freedman,* 380 U.S. at 58-59, *supra* notes 131-32 and accompanying text.

277. *Id.*

to stay this order pending appeal or to provide immediate appellate review.[278] Finally, to ensure that first amendment liberties are restrained no longer than is necessary to protect national security, a researcher whose publication has been restrained by a final court order should be able to reopen the order after a two-year period. At this court proceeding, the government again should have to prove its case, satisfying the same evidentiary requirements as required for the initial restraint. This two-year period would ensure that the threat to national security posed by a publication would be a continuing one, and that first amendment liberties would yield to national security interests only for so long as a threat to national security existed.[279]

VI

CONCLUSION

The Supreme Court affords Congress and the Executive broad deference in matters of national security. This is not a blind deference; the assertion of a national security interest, alone, does not justify infringement of individual liberties. While the protection of the nation's intelligence operations, including its cryptology systems, is a legitimate national security concern, the existing regulations intended to afford that protection are an unconstitutional prior restraint of cryptography publications because of their procedural deficiences. Further, the regulations are not within a national security exception to the first amendment, primarily due to the absence of congressional authorization and conflicting legislative histories. A prior review system cognizant of the first amendment could meet both the national security and individual liberties concerns inherent in public cryptography research. Careful and detailed statutory authorization of such a system is needed.

Kenneth J. Pierce

278. *See Nat'l Socialist Party,* 432 U.S. at 44, *supra* note 134 and accompanying text.

279. *Cf.* Chastleton Corp. v. Sinclair, 264 U.S. 546 (1923) (when a national emergency justifies governmental imposition of rent controls, controls can not exist beyond the emergency itself). To satisfy due process protections against government taking, the government may be required to pay compensation to a researcher whose publication is restrained. *See supra* note 6.

* *This Note has received the 1984 Earl Warren Prize, awarded by the Cornell Law School to the student who prepares the paper best exemplifying the late Chief Justice's commitment to civil rights.*