UIC John Marshall Journal of Information Technology & Privacy Law

Volume 4
Issue 3 *Computer/Law Journal - Winter 1984*

Article 5

Winter 1984

Nongovernmental Cryptology and National Security: The Government Seeking to Restrict Research, 4 Computer L.J. 573 (1984)

Christy Brad Escobar

NONGOVERNMENTAL CRYPTOLOGY AND NATIONAL SECURITY: THE GOVERNMENT SEEKING TO RESTRICT RESEARCH

I. INTRODUCTION

Laws restricting dissemination to foreign countries of cryptologic[1] devices and related technical data have been in effect since 1954.[2] The government places great emphasis on securing governmental communications and developing communication intelligence activities (electronic espionage).[3] Over the last twenty-nine years, this governmental interest and the resultant laws and regulations have spawned the belief that the government needs authority to control dissemination of cryptology information.[4]

For example, basic mathematical concepts having cryptology applications (technical data) can be encoded on microprocessing chips, effectively making cryptologic devices.[5] Fearing that national security will be threatened thereby,[6] the United States government has attempted to restrict dissemination of nongovernmental[7]

1. Cryptology is the scientific study of encoding and decoding messages as a means of rendering secure the information contained therein. It embraces cryptography and cryptanalysis. Cryptography refers to the process by which a message is rendered unintelligible to all but key holders. Cryptanalysis is the method by which a third party breaks a code or cipher without legitimately possessing the key. Encipher or encode is the process of transforming a message into a code. Decipher or decode describes the process by which the legitimate key holder applies the key to obtain the message that was sent. D. KAHN, THE CODEBREAKERS: THE STORY OF SECRET WRITING xii-xvi (1967).

2. *See* The Mutual Security Act of 1954, ch. 937, § 414, 68 Stat. 832, 848 (1954) (current version at 22 U.S.C. § 2778). *See also* 18 U.S.C. § 798 (1982).

3. D. KAHN, *supra* note 1, at 351-93.

4. *See infra* notes 46-65 and accompanying text.

5. *See infra* notes 88-89 and accompanying text.

6. Inman, *The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector*, 22 SIGNAL No. 6 (1979), *reprinted in* 3 CRYPTOLOGIA 129, 130 (1979).

7. *The Government's Classification of Private Ideas: Hearings Before a Subcomm. on Government Information and Individual Rights of the House Comm. on Government Operations*, 96th Cong., 2d Sess. 411 (1980) [hereinafter cited as *House Hearings*]. Author David Kahn has suggested that research outside the government be referred to as nongovernmental cryptology research rather than public cryptogra-

cryptology research, initially by attempting to fund that research[8] and currently by establishing a voluntary prior restraint on publication.[9]

The government believes that statutes, regulations and court cases give it the authority to restrict "technical data" that is significantly and directly related to defense articles;[10] one such defense article is the cryptologic device.

These desires and efforts by the government conflict directly with the nongovernmental cryptology researcher's need to publish, as well as his constitutional right to publish, which is guaranteed by the free speech clause of the First Amendment.[11]

This Note outlines the scope of the controls the government has over nongovernmental research in cryptology, examines how the government has applied these controls, and discusses the constitutionality of that application. It then suggests that the supposed controls on cryptology research are probably not warranted by statute and are probably unconstitutional as applied. This Note also suggests that, because of the increased dissemination of technology and the need of commercial enterprises to protect data bases and electronic communications,[12] the national security of the United States will be enhanced by encouraging nongovernmental research rather than attempting to restrict it.

II. OVERVIEW

A. History of Cryptology Development

Cryptology, in existence since early Egyptian times,[13] is generally regarded as within the governmental domain and is traditionally considered a state secret.[14] Like many nations, the United

---

phy. This will avoid confusion with public-key cryptography, a recent cryptographic breakthrough that could have significant commercial uses. In addition, the research is being done by private, not public individuals. He also suggested use of the term cryptology, which includes both the making and the breaking of codes and ciphers, as opposed to cryptography, which is used today to mean only the making of codes and ciphers. *Id.* This Note has adopted Kahn's suggestions.

8. *See infra* notes 46-54 and accompanying text.

9. *See infra* notes 55-63 and accompanying text.

10. *See infra* notes 66-102 and accompanying text.

11. U.S. Const. amend. I, cl. 2. *See also infra* notes 90-95 and accompanying text.

12. Inman, *supra* note 6, at 130.

13. David Kahn traces cryptology back to the first hieroglyphs sketched by scribes in the Egyptian town of Menet Khufu. D. Kahn, *supra* note 1, at 71.

14. Kahn, *The Public's Secrets*, 5 Cryptologia 20 (1981). The Bishop of Rochester, although protesting vehemently against a cryptanalyst's testimony regarding secret writings that linked him with an attempt to place a pretender on the throne of

States has had notable success with cryptology[15] and, since the National Security Agency (NSA)[16] was established, the United States has continued to invest untold sums in the work of communications intelligence and cryptography.

With the increased use of digital communication equipment, computers, and other electronic media in the private sector, a commercial market for cryptologic devices has developed to protect data bases and communications that are stored in or transmitted through this electronic network.[17] This commercial potential, coupled with breakthroughs by university scientists in basic mathematical concepts that have direct application to the cryptology field,[18] has led to an invasion of the governmental domain by nongovernmental researchers. According to NSA, the scientists' work threatens the secrecy of United States' codes and the communications intelligence work of NSA.[19] Consequently, using a national security justification often raised by the government in attempts to restrict first amendment rights,[20] NSA has attempted to extend available regulations to

---

England, was unable to question the process, as it was against the "public safety . . . to discover the Art or Mystery of Decyphering." *Id.*

15. D. KAHN, *supra* note 1, at 561-613.

16. NSA is one of the most secret arms of the United States intelligence divisions. It is responsible for the development of secure procedures and codes for government use and for the interception and cryptanalysis of foreign codes. It was so secret that, until 1962, NSA's existence was not acknowledged in the U.S. Government Manual. It wasn't until 1975 that the NSA director appeared before a congressional committee in public session. *See* H.R. REP. NO. 1540, 96th Cong., 2d Sess. 85 n.62a (1980) [hereinafter cited as HOUSE REP.].

17. Inman, *supra* note 6, at 131. *See also* HOUSE REPORT, *supra* note 16, at 112-13 (quoting J. Metelaki, *Telecommunications Privacy and the Information Society*, 2 TELECOMMUNICATIONS POLICY 4 (1978)).

> With the introduction of electronics to communications, codes which once consisted of written-letter substitution lists now involved special electronic circuitry to "scramble" the information content of message before sending and "descramble" it at the receiving end. Devices which perform this function have been developed to an extremely high level of sophistication by their respective government users to insure that equally sophisticated eavesdroppers who intercept the communications cannot, by computer analysis or other means, descramble the information. This scrambling or "encryption" technology has become so critical that it is handled as a state secret by each respective using government.

Id.

18. *See infra* notes 37-39 and accompanying text.

19. Inman, *supra* note 6, at 130.

20. *E.g.*, New York Times Co. v. United States, 403 U.S. 713 (1971) (The Pentagon Papers case); Snepp v. United States, 444 U.S. 507 (1980) (violation of employment contract by government agent by publishing book without submitting it to CIA for approval); Haig v. Agee, 453 U.S. 280 (1981) (revocation of passport of ex-CIA agent engaged in exposing current CIA agents); United States v. The Progressive, 467 F. Supp.

control nongovernmental research in cryptology.[21]

B. The International Traffic in Arms Regulation

The International Traffic in Arms Regulation (ITAR) was promulgated under authority of section 1934 of Title 22 of the United States Code, which has been superceded by section 2778 of the same title.[22] The new section restructured U.S. arms sales policies to provide for increased congressional supervision and review of all aspects of the foreign military sales program.[23] Nevertheless, Congress specifically delegated to the President the control of import and export of defense articles, defense services, and related technical data.[24] The power to develop and administer regulations under this statute was given to the Department of State. Pursuant to that authority, the ITAR was adopted.[25]

The first section of the ITAR sets out the U.S. Munitions List and designates various items as arms, ammunitions and implements of war.[26] Included are "speech scramblers, privacy devices, cryptographic devices (encoding and decoding) and specifically designed components therefor, ancillary equipment, and especially devised protective apparatus for such device, components, and equipment."[27] The statute and regulations indicate that, in order to further foreign policy objectives, export and import of these articles

990 (W.D. Wis. 1979) (imposing prior restraint on publication of a technical article on the hydrogen bomb).

21. Inman, *supra* note 6, at 134-35 (proposing that the current regulatory framework should be strengthened as to export of cryptologic devices and technical information; at the same time, basic research and scientific information should have free flow among scholars in different countries). *See also* Ungar, *The Growing Threat of Government Secrecy*, Tech. Rev., Feb.-Mar. 1982, at 33, 35 (discussing a bill introduced in the House of Representatives that would alter the Arms Export Control Act, 22 U.S.C. § 2778, to give the secretary of defense the power to restrict communications of any kind, including publication, unless withholding of that information is contrary to the national interest); *infra* notes 39-63 and accompanying text.

22. 22 U.S.C. § 2778 (1982). Section 1934 was incorporated into § 2778 by Pub. L. No. 94-329, § 212(b)(1), 90 Stat. 729, 745 (1976). The regulations promulgated under § 1934 were also continued under the new section. Pub. L. No. 94-329, § 212(b)(2), 90 Stat. 729, 745 (1976).

23. H.R. Rep. No. 1144, 94th Cong., 2d Sess. 8, *reprinted in* 1976 U.S. Code Cong. & Ad. News 1378, 1385.

24. 22 U.S.C. § 2778(a)(1) (1982).

25. 34 Fed. Reg. 12,029 (1969).

26. 22 C.F.R. § 121.01 (1982). Although the current regulations do not reflect the change in the statute wording from "arms, ammunitions and implements of war" to "defense articles and defense services," the Department of State is reportedly making that update.

27. 22 C.F.R. § 121.01(XIII)(b) (1982).

will be controlled by licensing.[28] Licenses are to be granted after considering "whether the export of an article will contribute to an arms race, or increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control arrangements."[29]

To accomplish these objectives, it is also necessary to control the dissemination of technical data. Without such control, de facto export of a restricted defense article could occur via disclosure of the technology necessary to build the article outside of the United States. Dissemination would thus occur without satisfying the licensing requirement, frustrating the foreign policy objectives of the ITAR.[30] It is difficult, however, to determine what knowledge or technical information is sufficient to effectually transfer one of these defense articles.[31] The ITAR opted for a broad definition of technical data that includes any classified information that could be used or adapted for use in the development of Munitions List items.[32]

This raises the issue of how broadly the term "technical data" can be construed. At some point the transfer of information is insufficient to facilitate development of the Munitions List item.[33] There is also a question, especially pertinent to cryptology restriction, of whether basic science research can be controlled by the technical data restriction requirement.[34]

Assuming that the information in question is within the "technical data" definition of the ITAR, another question raised by the ambiguity of the regulations is when does an "export" occur? According to the ITAR, technical data can be disclosed orally, visually or by documentation.[35] Export occurs whenever technical data

---

28. 22 U.S.C. § 2778(a)(1) (1982).

29. *Id.* at § 2778 (a)(2).

30. *See infra* notes 66-89 and accompanying text.

31. *See infra* notes 92-95 and accompanying text.

32. 22 C.F.R. § 125.01 (1982).

As used in this subchapter the term "technical data" means: (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; or (c) classified information as defined in § 125.02.

33. *See infra* notes 92-95 and accompanying text.

34. HOUSE REP., *supra* note 16, at 84-85. Basic scientific research is a domain traditionally thought to be unrestrictable because it is also discoverable by other researchers.

35. 22 C.F.R. § 125.03 (1982). The section in pertinent part reads:

These controls shall apply whenever the information is to be exported by oral, visual, or documentary means. Therefore, an export occurs whenever

is mailed, shipped, or carried by hand out of the United States, disclosed through visits abroad by American citizens, or disclosed to foreign nationals in the United States.[36]

A footnote to the general exemptions[37] (which exempt from ITAR control any technical information in published form and subject to public dissemination) indicates that appropriate governmental approval of any technical data falling within the definition of section 125.01, whether developed under government contract or privately, must be obtained by the party seeking publication.[38] This could subject domestic publication of technical data to the ITAR licensing requirements.

From the foregoing, it is clear that the government intended to restrict dissemination of technology relating to defense articles and defense services. Since the ITAR applies to cryptologic devices, the major question raised by the actions of NSA toward researchers in cryptology is the extent of the government's power to impose restrictions on researchers delving into basic scientific research. Such research, though privately developed, may be specifically applicable to the technology of items on the Munitions List.

In order to appreciate this problem, it is helpful to examine the government's attempts to influence research in the cryptology field.

---

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). A license to export technical data shall not be used for foreign production purposes, or for technical assistance in such production, without the specific approval of the Department of State.

36. *Id.*

37. 22 C.F.R. § 125.11 (1982).

Except as provided in § 126.01, district directors of customs and postal authorities are authorized to permit the export without a license of unclassified technical data as follows:

(1) If it is in published form and subject to public dissemination by being:
   (i) Sold at newstands 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. § 125.11(a)(1).

38. The burden for obtaining appropriate U.S. Government approval for the publication of technical data falling within the definition in § 125.01, including such data as may be developed under other than U.S. Government Contract, is on the person or company seeking publication.

22 C.F.R. § 125.11 n.3 (1982).

C. The Government's Attempt to Control Nongovernmental Cryptology

1. *Emerging Nongovernmental Research*

Two conditions have greatly encouraged research in cryptology by those outside government. First, the availability of communications and information on electronic digital equipment has emphasized the need for greater informational security.[39] Physically stealing information from a file cabinet is no longer necessary; one need only access the file remotely and copy it electronically.[40] To monitor electronic communications, one may set up powerful listening devices next to the microwave transmitter and eavesdrop. In addition to the increased need for secure systems, a decrease in the cost of computing power has made it cost efficient to use cryptologic devices to secure data and transmit communications safely.[41]

As these factors combined to increase the commercial potential of cryptologic devices, university computer scientists began making conceptual breakthroughs in basic mathematical theories. These were directly applicable to cryptology.[42] Foremost among these efforts was the development of public-key cryptography,[43] which allows publication of a key for the encoding of any message to a company. Once encoded, only that company has access to the private key that can decode the message. The advantage of this system is the decrease in the number of keys that are needed. Previously, companies needed separate keys for every combination of sender and receiver. Under the public-key concept, every sender uses the same public-key, presumably published in catalogue form, to send a message to that receiver. The receiver is able to decode the message because he has access to the mathematically related private-key, which decreases exponentially the number of computations needed to decode the message.[44]

---

39. Faflick, *Opening the "Trapdoor Knapsack,"* Time, Oct. 25, 1982, at 88.

40. Kahn, *Cryptology Goes Public*, 58 Foreign Affairs 141, 153 (1979).

41. Kahn, *supra* note 14, at 26.

42. Faflick, *supra* note 39, at 88.

43. *See* Diffie & Hellman, *Privacy and Authentification: An Introduction to Cryptography*, 67 IEEE Proceedings 397 (1979) (technical discussion of public-key cryptography with extensive bibliography); Rivest, Shamire & Adleman, *On Digital Signatures and Public Key Cryptosystems*, 21 ACM Comm. 120 (1978); Hindin, *Bell Algorithm Speeds Decryption of Public-key Coding Schemes*, Electronics, Aug. 11, 1981, at 39-40; Booth, *Authentication of Signatures Using Public-key Encryption*, 24 ACM Comm. 772 (1981).

44. Faflick, *supra* note 39, at 88. This Article describes the public-key concept as electronic mailboxes set up with two keys for each subscriber to the system. Dick Tracy, should he choose to subscribe, selects his own two keys, much as a bank permits customers to choose their own cash-machine passwords. If Buck Rogers wants

This and other new developments, and the professional literature they spawned, generated attempts by NSA to restrict research and publication by nongovernmental cryptology researchers. NSA was concerned that these nongovernmental efforts might allow other nations to use newer and more complex communication systems, significantly decreasing the signals communication effort (electronic espionage) of NSA. Continuing research also might threaten the security of government codes.[45]

2. *NSA's Attempt to Fund Nongovernmental Research*[46]

Much of the scientific research in cryptology is supported by grants from the National Science Foundation (Foundation). These grants are administered by the Division of Computer Research.[47] As early as 1975, the Foundation was aware that NSA felt it had sole statutory authority to fund research in cryptology.[48] On April 20, 1977, two representatives of NSA visited the Foundation to express concern over its funding of cryptology research. They indicated that NSA wanted to coordinate the funding of such research with the Foundation.[49]

At the same time, the Senate Select Committee on Intelligence, investigating allegations that NSA was improperly involved in the development of a data encryption standard, recommended that the Foundation and NSA attempt to reduce the ambiguity and uncertainty in the granting of research funds for nongovernmental cryptology.[50] As a result, Foundation Director Richard C. Atkinson suggested that NSA fund two or three million dollars of unclassified research at universities to alleviate the current problems.[51]

The first documented attempt to use this new policy occurred in August of 1980 when Leonard Adleman, a theoretical computer sci-

---

to send Dick Tracy a secret communication, he simply looks up Dick's public encoding key in a directory and uses it to garble his message. No one without access to Dick's secret decoding key, not even Buck himself, can read the resulting scramble of letters and numbers. *See also* Kahn, *supra* note 40, at 153-54.

45. *See* Inman, *supra* note 6, at 129; HOUSE REP., *supra* note 16, at 62-63; *House Hearings*, *supra* note 7, at 707-09.

46. For a detailed account, see HOUSE REP., *supra* note 16, at 77-85.

47. *House Hearings*, *supra* note 7, at 762 (memorandum from Division of Computer Research to Foundation General Counsel).

48. *Id.* at 763 (reply memo from General Counsel).

49. *Id.* at 764-65 (memo to Foundation file on visit of NSA representatives).

50. STAFF OF SENATE SELECT COMM. ON INTELLIGENCE, 95TH CONG., 2D SESS., UNCLASSIFIED SUMMARY: INVOLVEMENT OF NSA IN THE DEV. OF THE DATA ENCRYPTION STANDARD 4 (Comm. Print 1978) [hereinafter cited as INVOLVEMENT OF NSA IN THE DES].

51. *House Hearings*, *supra* note 7, at 770-71.

entist associated with the Massachusetts Institute of Technology and the University of Southern California, presented a proposal to do research involving the fundamental understanding of what it means for a computation to be hard or easy.[52] Adleman received a telephone call indicating that part of his grant proposal would not be funded by the Foundation. He learned later that portions of it were to be funded by NSA, to which he objected. Adleman indicated to colleagues that he did not want any implicit commitments to NSA and he wondered what would happen if NSA attempted to classify his work and he refused.[53] The Foundation eventually acquiesced and wholly funded his research. Many scientists, however, were left questioning the propriety of funding basic research through NSA. The research community was also left to contemplate where the study of cryptology ends and basic research in mathematics begins.[54]

3. *Limitations on Publication—Formation of the Public Cryptography Study Group*

Admiral Robert Inman, director of NSA, broke a twenty-five year agency policy of silence by giving an exclusive interview in 1978. He was motivated by publicity surrounding the imposition of the Invention Secrecy Act on patents sought for cryptologic inventions by nongovernment researchers.[55] During this interview Inman proposed that a dialogue be opened up between NSA and the academic community regarding the implications of new research in cryptography and communications security.[56] As a result, the Public Cryptography Study Group was formed, funded by a grant from the Foundation.[57]

The minutes to the various meetings indicate that, for discussion purposes, the members of the committee accepted the proposition that public cryptography might, under some circumstances, imperil national security. That proposition was taken on faith because of security restrictions.[58] After a broad initial discussion, it

52. Kolata, *Cryptography: A New Clash Between Academic Freedom and National Security*, 209 SCIENCE 995 (1980).

53. *Id.* at 995-96.

54. *Id.* at 995.

55. Shaply, *NSA Slaps Secrecy Order on Inventors' Communications Patent*, 201 SCIENCE 891 (1978). *See also* Mark, *The Patent Secrecy Act of 1952*, 15 COLUM. J.L. & SOC. PROBS. 359 (1980).

56. Shaply, *Intelligence Agency Chief Seeks "Dialogue" with Academics*, 202 SCIENCE 407 (1978).

57. *House Hearings*, *supra* note 7, at 700-01.

58. *Id.* at 703.

was determined that "the core . . . question before the committee was whether some form of prior restraint on publication of research results and other information relating to cryptology [was] necessary, feasible, and desirable."[59]

The committee appointed a subcommittee to consider the feasibility issue.[60] This subcommittee proposed a voluntary approach which was subsequently implemented. The program relied on a narrow definition of potentially classified cryptology information. Authors and publishers would be asked to voluntarily submit prospective articles containing such information to NSA for review. If the article did not contain objectionable information, or if the questions that arose were resolved satisfactorily, publication would proceed. If there were disagreements, however, an advisory committee, made up of five members with security clearance—two from NSA and three from the academic community—would recommend to the Director of NSA whether the government should attempt to restrain publication. The director would not have to follow the recommendation.[61]

Voluntary participation in the program is not universal.[62] In at least one instance, however, the dialogue between NSA and a researcher led to a delay in publication to allow other researchers time to catch up with the major advance that the paper presented.[63]

4. *Summary—Control of Nongovernmental Research*

These examples show NSA's concern with and actions toward the development of nongovernmental research. It may be impossible for NSA to obtain control of that research;[64] however, by impeding the speed with which scientists develop and disseminate ideas, it may manage to maintain its scientific lead.[65] The ultimate test—a showdown between NSA and a researcher, when the interest of NSA in national security and the interest of the researcher in publication of his work come in direct conflict—has yet to be reached.

---

59. *Id.*

60. *Id.* at 704.

61. HOUSE REP., *supra* note 16, at 97 n.99.

62. Kolata, *MIT Committee Seeks Cryptography Policy*, 211 SCIENCE 1139 (1981).

63. Wallich, *Cryptography: Voluntary Control Seems to Work*, IEEE SPECTRUM, May 1982, at 66.

64. *House Hearings*, *supra* note 7, at 702 (indicating NSA believed that the present statutory controls prevent them from controlling scholarly papers, research and conferences). *But see infra* notes 88-89 and accompanying text (indicating that there is little difference between basic research and application in the computer science research field).

65. Kolata, *supra* note 62, at 66.

Whether the government has authority to enjoin publication of that research under the Arms Export Control Act or the Espionage Act will be discussed next.

III. STATUTORY INTERPRETATION

A. The Scope of the "Technical Data" Definition

The central question about the ITAR that this Note addresses is whether "technical data" was intended to include research that has direct application to cryptology, but is not directly related to a specific device on the Munitions List. This is the crucial question in determining whether NSA, following the procedure outlined by the Public Cryptography Study Group, may enjoin a scientist from publishing his research. The history of the Munitions Act casts doubt upon NSA's ability to do so, although court interpretations may allow such action.

1. *Legislative History—Section 1934*

Section 1934 of Title 22 of the United States Code was enacted as part of the Mutual Security Act of 1954.[66] It was included in the Act at the request of the executive department to tighten controls on the export and import of munitions and to alleviate the burden of paper work that was required of commercial enterprises under the previous legislation.[67]

Initially, the bill before the House did not contain any reference to technical data. The addition was first suggested in the House hearings in order to strengthen the bill to allow for control of the dissemination of technical data that would enable items on the Munitions List to be built outside the country. It was suggested that "drawing, design data, specifications, and standards pertaining to such articles" be included in the statute, or that it be made clear in the legislative history that these items were included in the meaning of "arms, ammunition and implements of war."[68]

The Senate version of the bill, after describing items subject to control, added the words "and technical data relating thereto." The conference committee, admitting the difficulty of administering such a provision except when wartime censorship was in effect, nevertheless felt it was important that those responsible for controlling ex-

66. Ch. 937, § 414, 68 Stat. 832 (1954).

67. *See* H.R. Rep. No. 1925, 83d Cong., 2d Sess., pt. 1, at 89 (1954).

68. *Hearings on H.R. 6344 Before a Subcomm. of the House Comm. on Foreign Affairs*, 83d Cong., 2d Sess. 11-14 (1954) (testimony of Col. C.K. Moffatt).

ports and imports of munitions have this authority.[69]

The legislative history indicates that the initial inclusion of "technical data" in the statute envisioned a direct link between the technical data exported and production of an article on the U.S. Munitions List. Only if that relationship existed would technical data be subject to the regulations promulgated under authority of the statute.

2. *Legislative History—Section 2778*

The legislative history of 22 U.S.C. § 2778, which replaced section 1934, added nothing new to aid in interpreting the meaning and intent of "technical data." The new Munitions Control statute was amended and included in a larger bill, The International Security Assistance and Arms Export Control Act of 1976.[70] The purpose of this bill was to bring all the statutory controls on arms exports and imports under one act, the Arms Export Control Act.[71]

The new section restated most of section 1934, but changed "arms, ammunitions, and implements of war" to "defense articles and defense services," to conform to the language of other sections of the new Act.[72] The new Act included a savings provision for regulations issued under the previous statute.[73]

By that time, however, control of technical data was apparently more readily acceptable to Congress. In describing the effects of the Act, the Senate Report emphasized that technical data relating to defense articles and defense services were subject to Presidential control; specific items could be designated by the President as items requiring a license for export. There was no debate about the scope of "technical data."[74]

Although the history of the Munitions Control statute implies a narrow interpretation of "technical data," the statute, on its face, does not dictate such a limited view. There is no indication why Congress substituted the broader term "technical data related thereto" for the phrase "drawings, design articles, specifications and standards pertaining to such articles."[75] The definition of technical data incorporated into the ITAR included much more than the four items originally suggested.[76] The courts, in the two decisions involv-

69. H.R. REP. No. 2637, 83d Cong., 2d Sess. 44 (1954).
70. Pub. L. No. 94-329, 90 Stat. 729 (1976).
71. S. REP. No. 876, 94th Cong., 2d Sess. 42 (1976).
72. *Id.*
73. Pub. L. No. 94-329, § 212(b)(2), 90 Stat. 729, 745 (1976).
74. S. REP. No. 876, *supra* note 71, at 42-43.
75. *See supra* notes 68-69 and accompanying text.
76. 22 C.F.R. § 125.01 (1982). See *supra* note 32 for text of that definition.

ing the ITAR,[77] accepted the broader definition. It can be argued that these courts have extended the definition to allow control over the export of mathematical research having direct application to cryptology.

3. *The Court Cases*

a. United States v. Van Hee

In *United States v. Van Hee*,[78] the court concluded that the general technical knowledge and experience of United States citizens is included in the technical data definition, and thus, is subject to the licensing requirements of the ITAR. The case involved the sale of armored amphibious vehicles to Portugal. When Portugal would not certify that they would be used only in Portugal, the State Department revoked the export license it had originally granted to the corporation for which Van Hee worked. Van Hee and the chief engineer of the corporation subsequently recruited Americans to go to Portugal and construct a similar armored amphibious vehicle for that country. Van Hee was convicted of conspiring to violate the Munitions Control Act.

The first issue on appeal was whether the defendants had taken and used any "technical data" while building the amphibious vehicles in Portugal.[79] Blueprints and general technical knowledge and experience were held by the court to be included within the technical data definition of the ITAR.[80] The court relied upon the broadness of the ITAR definition, implying that general technical knowledge was "similar information which could enable the recipient to use, produce, operate, maintain, repair, or overhaul the article to which these data relate."[81] As long as the information would enable the recipient to develop a Munitions List item, it seems it is "technical data" according to the court in *Van Hee*.

77. United States v. Van Hee, 531 F.2d 352 (6th Cir. 1976); United States v. Elder Indus., 579 F.2d 516 (9th Cir. 1978).

78. 531 F.2d 352 (6th Cir. 1976). For an in depth review of *Van Hee* suggesting that the court should not have expanded technical data to include general technical knowledge and know-how, see 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 LAW & POL. 91 (1976).

79. *Van Hee*, 531 F.2d at 355.

80. *Id.* at 356-57.

81. *Id.* at 356 (quoting 22 C.F.R. § 125.01 (1966)). The definition in the regulations has been changed, using more general language. See *supra* note 32 for text of 22 C.F.R. § 125.01 (1982).

b. United States v. Elder Industries

United States v. Elder Industries[82] restricted the technical data definition to data significantly and directly related to specific items on the U.S. Munitions List. After an export license had been denied, Elder Industries continued to consult with French missile firms regarding techniques for creating durable lightweight materials. These materials could be used for nozzles on rockets and missiles, but they also had non-military applications.

The court reversed the conviction, because the trial court excluded evidence showing that the technology had applications in areas other than munitions. The appellate court found that the evidence was relevant to whether the defendant knew or should have known that the recipient of the exported information would use it to produce a Munitions List article.[83] In addition, the appellate court felt the defense should have been allowed to develop the proposition that the information and assistance given was not sufficient to enable the French missile firms to manufacture rocket nozzle components. It indicated that the key issue is the close relationship between the information and the Munitions List items.[84] This case can be read to restrict "technical data" to data which will lead to development of a specific Munitions List item.

Although *Elder Industries* limits the definition of technical data, the definition is still broader than the one originally intended, as indicated by the legislative history.[85] No specific missile components or plans for building them were exported by Elder Industries. Only the technique, transferred by demonstration and experimentation, was involved.[86] In *Elder Industries*, the court implied that, if the transfer of information is sufficient to allow the recipient to produce a Munitions List item, the technology is subject to the ITAR controls.[87]

Technical data is not transferred in a vacuum, however. If the recipient has knowledge that, combined with the data transferred, may be sufficient to produce a Munitions List item, then a transfer of technology "significantly and directly related" to a Munitions List item has occurred, and the test in *Elder Industries* has been met. The data transferred is thus subject to the licensing provision.

---

82. 579 F.2d 516 (9th Cir. 1978).

83. *Id.* at 522.

84. *Id.*

85. *See supra* notes 66-69 and accompanying text.

86. *Elder Indus.*, 579 F.2d at 518-19.

87. *Id.* at 522.

4. *Summary—"Technical Data" Definition*

Applying the ITAR "technical data" definition, as interpreted by the courts, to current cryptology research confirms the belief that the ITAR can control export of basic scientific research. Pure research is normally judged to be uncontrollable since, by definition, it is discoverable by any other scientist. Admiral Inman implied as much when he indicated that it is the application of the basic mathematical theories, not the theories themselves, that should be restricted.[88] Professor George Davida stated that, in computer science research, there is little difference between theory and application. "[W]ith development of microprocessors it becomes trivial to take a procedure that someone develops theoretically and turn it into a machine that can encrypt."[89] If Davida is correct, the ITAR "technical data" definition allows NSA to restrict export of cryptology research. The reasoning is as follows: Basic mathematical research relating to cryptology can lead to production of cryptologic devices. Since that basic research is "significantly and directly related" to a Munitions List item, it qualifies as "technical data." Thus, export of the research can be restricted.

Since this research may, if it is exported, be subject to regulation by the ITAR, the next step is to determine when a publication qualifies as an export.

B. When Does an "Export" Occur?

As previously discussed,[90] an export of information occurs when information is disclosed to foreign nationals by oral, visual, or documentary means, whether the foreign nationals are within the United States or abroad. The regulations imply that any technical data must receive governmental approval prior to publication, even in a domestic source. The requirement of governmental approval is aimed at preventing the willful violation of the ITAR. For example, a researcher could publish the information domestically, then rely upon the domestic publication exemption to justify export to foreign nationals.[91]

As written, the regulation drastically intrudes upon communications between scientific colleagues. In American universities, an informal communication network has developed. Long before a paper is published in a journal, working papers, preprints and personal

88. *House Hearings*, *supra* note 7, at 427.

89. *Id.* at 428.

90. *See supra* notes 35-38 and accompanying text.

91. 22 C.F.R. § 125.11 (1982) (see *supra* note 37 for text). The exporter must claim the applicable exemption before it will take effect. *See* 22 C.F.R. § 125.22 (1982).

communications have already dispersed the information to the researcher's colleagues.[92] Control of research results would require control of this informal network, an almost impossible task.

In addition, over one-third of the graduate students involved in computer science studies are foreign nationals.[93] The ITAR, strictly applied, would prevent communication between students and faculty or between university colleagues; dispersal of research information to these foreign students and faculty members, via the informal communication network, would constitute export.

Although domestic publication may seem to be exempt from ITAR controls,[94] most scientific journals include foreign nationals among their subscribers. Publication in these journals would fall within the ITAR export definition. Thus, the constant worldwide communication among scientists makes almost any publication or dissemination of "technical data" an export subject to the restrictions of the ITAR.[95]

In summary, historically it is extremely doubtful that the framers of the Munitions Control statute intended or anticipated governmental restriction of basic nongovernmental scientific research, such as is presently occurring in the cryptology field. Nevertheless, the ITAR, as interpreted by the courts, allows NSA to restrict export of that research, which conceivably includes communications between foreign students, their teachers, and the teachers' foreign scientific colleagues.

C. Espionage Controls Over Nongovernmental Cryptology Research

Admiral Inman expressed, as one of his major concerns, that continual research into cryptology might lead to effective attacks on governmental codes, thereby significantly harming national security.[96] Thus, an additional basis for restricting this research may be the espionage provisions found at section 798 of Title 18 of the

92. Gray, *Technology Transfer at Issue: The Academic Viewpoint*, IEEE Spectrum, May 1982, at 64, 65; Letter from Prof. Richard Mandelbaum to Science Magazine, 210 Science 960, 962 (1980).

93. Ungar, *supra* note 21, at 33.

94. *See supra* notes 37-38 and accompanying text.

95. U.S. Dep't of Commerce, Export Ad. Rep. app. D 134 (1977). Mere publication of data is generally an ineffective means of transferring knowledge. Effective technology transfer depends largely upon the degree of interaction between those providing and those receiving the data. *Id*. *But see supra* note 89 and accompanying text (suggesting that with respect to cryptology, publication of data does transfer sufficient knowledge to produce a cryptographic device).

96. Inman, *supra* note 6, at 131-32.

United States Code.[97]

The legislative history of this espionage statute suggests that it was passed to eliminate a loophole, which allowed former government employees who were no longer subject to the security controls (primarily Executive Orders) applicable during their employment, to reveal classified information without the threat of a penalty.[98]

In fact, one of the primary reasons this espionage statute was enacted was the disclosure by the former head of U.S. government cryptology that Japanese codes had been broken by the U.S. government. The inability of the U.S. to break the more complex codes that the Japanese developed as a result of that security leak contributed to the success of Japan's surprise attack at Pearl Harbor.[99]

The restriction pertinent to nongovernmental research in cryptology is narrowly written. The conduct that violates it is confined to revealing a code or cryptologic device of the government.[100] The statute is applicable if that information is knowingly and willfully revealed, regardless of where it was developed. If Admiral Inman is correct (that continual research and publication of cryptanalysis methods may reach into the domain of already developed government codes), this statute would be available to restrict dissemination of such information.[101]

This may be a more permissible form of control than that discussed under the ITAR. It requires a present national security risk rather than a potential future effect. It is not clear, however,

---

97. 18 U.S.C. § 798 (1982).

98. S. REP. No. 111, 81st Cong., 1st Sess. 2-4 (1949). Although there were two acts protecting cryptology information at the time (the Espionage Act of 1917 and the Act of June 10, 1933), neither effectively prevented disclosure of government codes and ciphers by former government workers. The discussion of the bill indicates that the previous bill, enacted on June 10, 1933, was passed in order to prevent a former government employee from publishing a second book. The first book had led to the changing of the Japanese diplomatic codes. *See also* D. KAHN, THE CODEBREAKERS, *supra* note 1, at 361-69.

99. S. REP. No. 111, *supra* note 98, at 3-4.

100. Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction . . . of any device . . . used . . . by the United States . . . for cryptographic or communication intelligence purposes. . . . Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

18 U.S.C. § 798 (1982).

101. Inman, *supra* note 6, at 131-32.

whether section 798 was intended to apply to researchers who were not entitled to classified information, but developed the same information by their own efforts. Presumably, given the threat to national security, the statute would apply to anyone who willfully and knowingly revealed the information, regardless of his source.

The intent requirement in the statute would probably preclude granting an injunction or convicting a nongovernmental scientist. In order to willfully and knowingly reveal a secret, the scientist must first know that it is a secret. With the present voluntary restraint system, the government could learn of the article prior to publication, but would have to advise the author that the information was classified in order to obtain an injunction.[102]

D. Summary—Statutory Interpretation

Given the close link between basic computer science research and the ability to create a cryptologic device from it, nongovernmental cryptology research easily fits within the ITAR's definition of "technical data." The research is thus subject to licensing requirements of the ITAR. Because of the broad dissemination of research information by scientists on the frontiers of their fields, either through prepublication communications or through the publication itself, the information is effectually transferred to foreign nationals, a violation of the ITAR if unlicensed. In addition, if the information to be published will reveal a solution or break a U.S. code, the government may be able to enjoin publication of the article by use of the espionage statute.

These potential restrictions on the researcher's ability to publish lead to questions of the constitutionality of these statutes and regulations as they apply to cryptology research, since communication of basic research seems well within the confines of the First Amendment protection on speech.

IV. CONSTITUTIONAL ISSUES

If technical data controls in the ITAR are read to include basic research[103] in cryptology by nongovernmental researchers, then constitutional claims arise. Given that broad interpretation, the ITAR may allow an administrator too much arbitrary and discretionary power, thereby subjecting the regulations to invalidation on

102. This assumes that the government has a proprietary interest in the information. The point is debatable, but, because the information can qualify as an export under the ITAR, it is not significant to this Note. For further information on this subject see House Rep., *supra* note 16, at 118.

103. *See supra* notes 66-89 and accompanying text.

overbreadth grounds. In addition, since the regulations place the burden of obtaining prior governmental approval on the party wishing to publish,[104] there may be a prior restraint issue. These were, in fact, the two constitutional issues raised by the defense in *United States v. Elder Industries*[105] and partially resolved by the Ninth Circuit. In addition, the government may rely on a time, place, and manner argument not raised in *Elder Industries*, claiming that the ITAR is lawful because it regulates conduct and only incidentally restricts speech.

A. OVERBREADTH

1. *The General Doctrine*

The constitutional doctrine of overbreadth applies when a given law, although valid in some applications, affects expressive activity to such a degree that, as applied in a given situation or in its entirety, it violates the First Amendment.[106] Overbroad laws are deemed unconstitutional because of the "chilling effect" they have on speakers.[107] The chilling effect results from the statute's broad reach into expressive areas; speakers who are otherwise constitutionally able to speak fail to do so because of the threat of prosecution or conviction under the law. To counteract this harm to one's right to speak, the Supreme Court has developed two approaches to overbreadth.

The first approach is the "as applied" test. It allows a law to operate where it might do so constitutionally, but vindicates the claim-

---

104. 22 C.F.R. § 125.11 n.3 (1982). *See supra* note 38 for text.

105. 579 F.2d 516 (9th Cir. 1978).

106. NAACP v. Alabama, 377 U.S. 288, 307 (1964). Justice Harlan, writing for the court, indicated that "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." *See also* G. GUNTHER, CONSTITUTIONAL LAW—CASES AND MATERIALS 1186 (10th ed. 1980).

107. The "chilling effect" has become a part of the First Amendment rubric. It generally describes the impact a law has on parties who, because they are unable to determine the scope of a law, would rather not speak than risk prosecution or protracted litigation. *See, e.g.*, Schaumburg v. Citizens for a Better Environment, 444 U.S. 620, 634 (1980). There the Court stated:

> Given a case or controversy, a litigant whose own activities are unprotected may nevertheless challenge a statute by showing that it substantially abridges the First Amendment rights of other parties not before the court. In these First Amendment contexts, the courts are inclined to disregard the normal rule against permitting one whose conduct may validly be prohibited to challenge the proscription as it applies to others because of the possibility that protected speech or associative activities may be inhibited by the overly broad reach of the statute.

Id. (citations omitted.)

ant who establishes that his own conduct is within the First Amendment and should not be subject to the burden of the law as it was intended.[108] In using the "as applied" analysis, the Court considers the particular facts before it; it does not adjudicate in the abstract.[109] It can balance the governmental interests against the damage to speech interests and, if warranted, narrow the statute by interpretation to prevent the restriction of constitutionally protected activities. Essentially, it carves out the impermissible reach of the statute.

The second overbreadth approach is a facial attack that results in complete invalidation of the law. It is based on sweeping and improper applications of a given law, which result from improper drafting of legislation.[110] This drastic measure is seldom used. Generally, it is used only to overcome conflict with and to protect valid First Amendment rights. Because of the value inherent in First Amendment rights and the "chilling" effect of such broad legislation on third parties, a litigant may raise the claims of third parties not before the court in seeking to invalidate a statute by this approach.[111]

To mitigate the force of facial invalidation of laws by the overbreadth doctrine, the Supreme Court, in *Broadrick v. Oklahoma*,[112]

---

108. Note, *The First Amendment Overbreadth Doctrine*, 83 HARV. L. REV. 844 (1970). The factors the court considers in an "as applied" analysis include:

> the degree to which the complainant's activity is within the concern of the amendment because oriented to communication of ideas; the degree of harm to valid governmental or social interests caused or threatened by the conduct at issue; how restrictive or punitive the interference; how weighty the policy said to justify interference, and how closely the policy is connected with the actual application of the statute. Whether the Court weighs all of these factors in each case or articulates and applies a general rule of privilege focusing on only certain of them, its task is closely bound to an examination of the particular conduct before it.

Id. at 844-45.

109. The Court normally requires parties before it to litigate only claims based on the facts before the Court. Broadrick v. Oklahoma, 413 U.S. 601 (1973). The Supreme Court has, however, relaxed these "standing rules" in a few contexts, when a countervailing policy requires that a litigant be allowed to bring claims of third parties not before the court. *See, e.g.*, Carey v. Population Servs. Int'l, 431 U.S. 678, 683 (1977); Craig v. Boren, 429 U.S. 190, 195 (1976). The Court has relaxed its standing rules with respect to overbreadth claims. The countervailing policy is the chilling effect of the statute on third parties. *See, e.g.*, Bigelow v. Virginia, 421 U.S. 809 (1974); Eisenstadt v. Baird, 405 U.S. 438 (1972).

110. Note, *supra* note 108, at 845.

111. When a law is invalidated by a facial overbreadth attack, the whole law, as applied to anyone, is invalid. Even a party whose conduct is within the valid reach of the statute cannot be prevented from engaging in that activity. *See* Note, *supra* note 108, at 845.

112. 413 U.S. 601 (1973).

applied a substantial overbreadth test to a state statute. The Court implicitly found that, in specific areas, such as the wearing of political buttons or displaying of bumper stickers, a restrictive state statute may overreach into protected political expression.[113] In balancing the need for breathing space in the First Amendment against the governmental objective (avoiding the political partisanship of government employees campaigning for their superiors), however, the Court required "that the overbreadth of a statute must not only be real, but substantial as well, judged in relation to the statute's plainly legitimate sweep."[114]

Further emphasizing its reluctance to invalidate laws, the Court has indicated that federal legislation should be saved from facial invalidation based on overbreadth whenever it is possible to constitutionally narrow the construction and remain consistent with legislative intent.[115]

2. *Overbreadth, Cryptology, and the ITAR*

In *Elder Industries*,[116] the Ninth Circuit discussed the issue of overbreadth in the ITAR and concluded that the regulations were not facially overbroad. It determined that the ITAR regulated conduct rather than speech. The government was thereby allowed to

---

113. *Id.* at 609-10.

114. *Id.* at 615. Although *Broadrick* held that the substantial overbreadth test applies particularly "where conduct and not merely speech is involved," in a recent case substantial overbreadth was extended to pure speech contexts as well. New York v. Ferber, 102 S. Ct. 3348 (1982) (court will not facially invalidate child pornography statute that is not substantially overbroad).

In addition, at least two commentators believe that the overbreadth case law can be distinguished by the type of statute involved. Three types have been noted. The test requires more overbreadth in the first two types of statutes than in the last. They are:

> 1) "censorial" laws which operate to burden the advocacy of definable viewpoints on matters of public concern; 2) "inhibitory" laws which impinge on expressive and associational conduct but whose impact tends to be neutral as to viewpoints sought to be advocated; 3) "remedial" laws which hamper first amendment activities for the purpose of promoting values which are within the concern of the amendment.

Note, *supra* note 108, at 918; J. NOWAK, R. ROTUNDA & J. YOUNG, CONSTITUTIONAL LAW 725-26 (1978).

115. *Broadrick*, 413 U.S. at 613. *See also* Erznoznik v. City of Jacksonville, 422 U.S. 205, 216 (1974). Three alternative approaches are suggested for courts to use prior to facially invalidating a statute. These are (1) degree of overbreadth (similar to the substantial overbreadth of *Broadrick*); (2) area of impact (a requirement that the challenged law must substantially involve First Amendment interests); and (3) adjudicatory alternatives (the carving out of impermissible areas of a statute). Note, *supra* note 108, at 858-65.

116. 579 F.2d 516 (9th Cir. 1978).

"pursue its legitimate objectives even though incidental limitations on expression may result."[117] The court limited the technical data definition to data "directly relevant to the production of a specified article on the Munitions List," by relying on the legislative history and a close reading of the regulations.[118] In addition, the court read an intent requirement into the technical data licensing process, indicating that "if the information could have both peaceful and military applications . . . the defendant must know or have reason to know that its information is intended for the prohibited use."[119]

This interpretation is consistent with the overbreadth doctrine. The regulations are narrowly interpreted to make them constitutional, in order to avoid facial invalidation.[120] The Ninth Circuit did not, however, discuss the initial decision it made in *Elder Industries*: that the ITAR sought to control conduct, not speech.[121] This decision allowed it to employ a less stringent constitutional test.[122] If the cryptology scenario described in the statutory section of this Note was presented to the courts, they might well take a fresh look at the facial invalidation argument and use a more stringent review because of the speech values implicated. That could result in declaring the ITAR unconstitutional.

The better view, however, is that the *Elder Industries* court was correct; regulating the control of international arms traffic does encompass mostly conduct. Since the court was able to narrow the technical data definition to avoid First Amendment problems, it should continue to refine the statute to avoid facial overbreadth challenges.

This is not the end of the overbreadth challenge, however. If the statute is not substantially overbroad when narrowly construed

---

117. 579 F.2d at 521.

118. *Id.*

119. *Id.*

120. *See supra* note 115 and accompanying text.

121. 579 F.2d at 520.

122. *House Hearings*, *supra* note 7, at 277 n.16 (Department of Justice memo). Prior to the Ninth Circuit decision in *Elder Industries*, but after oral argument, it was suggested that, although much of the ITAR was a regulation of conduct, the technical data provision, on a "cursory reading," involved communication and required a stiffer test than the test based on conduct.

This statute, if interpreted in terms of the three types of statutes set out *supra* note 114, would have been classified by the Court as a "remedial" law which only hampers First Amendment activity while promoting other values. The Department of Justice may have felt it was "censorial" or at least "inhibitory" because, on a "cursory reading," it impinges on expressive conduct. The court did not reach the substantial overbreath question, however, preferring to narrow the statute by interpretation to avoid these issues.

(it has few areas in which it impermissibly impinges on the freedom of speech), then it will be applied, as interpreted, in any subsequent litigation. The defendants in such litigation can still raise an "as applied" attack, which will whittle down the statute on a case-by-case basis. In this way, when regulating conduct is its ultimate aim, the statute will not impinge on free speech more than is permissible.[123]

Applying the ITAR to nongovernmental cryptology research leaves an opening for the "as applied" argument to succeed. Most researchers simply publish their findings, often to fulfill a requirement of the grant enabling them to conduct the research. The problem, as pointed out earlier, is that pure research collapses into applied research in the cryptology field, so that any publication could be an export of technical data.[124] Thus, the research may be "directly relevant" to the production of cryptology devices and meet the first part of the *Elder Industries* test.[125]

The intent requirement established by the Ninth Circuit in *Elder Industries* would not be met, however.[126] Since computers are in the forefront of communications today, developing safe codes for use by either business or government requires the same effort. If a literal interpretation is given to the intent requirement, nongovernmental scientists need only indicate they are publishing to further the business applications of cryptology and deny any intention to provide information for military applications in order to avoid application of the ITAR. In fact, given the *Elder Industries* interpretation, a scientist could sell cryptology information to a foreign bank (for example, to secure electronic wire transfers of funds) without obtaining a license and without violating the ITAR, since this is a peaceful rather than a military application. There might be danger to United States security in this, because of the ease with which a foreign military government could obtain information from its industries. This demonstrates that, even if the publication of cryptology research is a threat to national security and its dissemination can be classified as an export under the ITAR, it will be difficult to prove that, by publishing basic scientific research data, the researcher was intentionally providing information for military use. Under *Elder Industries'* "as applied" overbreadth analysis, the dual use of cryptology research and the nongovernmental scientist's avowed purpose to develop commercially feasible cryptology systems prevent government restriction.

123. *See infra* notes 148-61 and accompanying text.

124. *See supra* note 89 and accompanying text.

125. *See supra* text accompanying note 82.

126. *See supra* text accompanying note 83.

Unlike the *Elder Industries*' nozzle technology, which had other distinct nonmilitary applications, nongovernmental cryptologic devices can be used by both the military and private industry. A scientist's intention that his research be used in the private sector does not prevent its cryptologic use in the military area. This casts doubt on the validity of applying the intent requirement of *Elder Industries* to nongovernmental cryptology research since it does not distinguish between these cryptology applications.

It is doubtful, however, that any test a court devised would distinguish between different users when they use the same cryptologic device in the same manner. The courts should either apply the intent requirement of *Elder Industries*, allowing dissemination of nongovernmental cryptology research, or reassess the weights of the arguments to determine if a restriction on permissible speech (dissemination of nongovernmental research for private use) is outweighed by the harm to governmental security if the nongovernmental cryptology research is disseminated. The latter position, however, is exactly what courts seek to avoid.[127] If that trend is followed, overbreadth analysis would seem to allow dissemination of nongovernmental cryptologic research as speech activity protected by the First Amendment and not subject to the burden of the ITAR "technical data" definition.[128]

B. Prior Restraint.

In *Elder Industries*, the court summarily disposed of the prior restraint issue on the same grounds as the overbreadth claim,[129] without noting that the facts did not explicitly raise this issue. The court might have decided differently had it been faced with a fact situation in which an individual wished to publish privately developed technical information relating to a Munitions List item.

---

127. There have been no specific overbreadth cases in which the Supreme Court balanced national security interests against First Amendment freedoms, but the Court has, in a few cases, balanced other governmental interests against First Amendment freedoms. *See*, *e.g.*, Keyishian v. Board of Regents, 385 U.S. 589 (1967) (invalidating state statute aimed at preventing the appointment of subversives in state employment); Colten v. Kentucky, 407 U.S. 104 (1972) (upholding a statute aimed at preventing disorderly conduct when no bona fide intention to exercise a constitutional right existed). *But see* United States v. Robel, 389 U.S. 258 (1967) (federal statute sought to prevent a member of a Communist-action organization from engaging in employment at any defense facility; the Court refused to balance the governmental interest against the defendant's First Amendment rights, ruling that the legislation must be drawn more narrowly to avoid the conflict). *See also* Annot., 45 L. Ed. 2d 725, 742-743 (1976).

128. *See supra* note 108 and accompanying text.

129. 579 F.2d at 521.

1. *The General Doctrine*

A prior restraint generally takes one of two forms.[130] Historically, authors were required to obtain licenses prior to publication of their work. This type of restraint has been rejected since it was outlawed in England in 1694.[131] A form of prior restraint commonly used today is the court imposed injunction.[132]

Prior restraints have been distinguished from subsequent licensing systems and civil damage awards on the basis of timing: prior restraints prohibit an action prior to its occurrence, while licensing and damage awards punish after the occurrence of an event. Both prior restraints and subsequent punishments, however, are meant to deter speakers or publishers from engaging in harmful acts in the future.[133]

If the government, implementing a prior restraint system, fails to discover a violation prior to publication, and nevertheless punishes the scientist, there is little difference between the two systems.[134] Although there may be little doctrinal difference between prior and subsequent restraints, the government would probably prefer to entirely prohibit publication of sensitive information, in order to prevent any disclosure to the audience.

A distinction was made, however, in *Walker v. City of Birmingham*.[135] The United States Supreme Court prevented the defendants from raising constitutional claims that, by the Court's own admission, were valid. It held the defendants liable for contempt of court when they failed to comply with an injunction issued by the lower court. Thus, the defendants were unable to raise constitu-

130. Blasi, *Toward a Theory of Prior Restraint: The Central Linkage*, 66 MINN. L. REV. 11, 14-15 n.17 (1981) (listing numerous regulatory procedures that might fit within a functional definition of "prior restraint").

131. J. NOWAK, R. ROTUNDA & J. YOUNG, *supra* note 114, at 713.

132. The seminal case in American constitutional law invalidated as a prior restraint an injunction designed to abate a newspaper as a public nuisance. Near v. Minnesota, 283 U.S. 697 (1931).

133. Blasi, *supra* note 130, at 11. Blasi forcefully argues that injunctions and prior licensing systems have common factors not found in subsequent restraints that distinguish between the two systems. Although agreeing with the majority of commentators that timing of the restraint and self-censorship are not distinguishing factors, Blasi feels prior restraints are overused, lead to adjudication in the abstract, influence audience reception, and expand government powers in ways not shared by subsequent penalty systems.

134. If the government has no notice of the publication or speech, it cannot restrain it. Thus, violation of the law would occur, but the government would be unable to punish the act until afterward, effectively turning a prior restraint into a subsequent penalty.

135. 388 U.S. 307 (1967).

tional claims that would have been available if the penalty had been a subsequent restraint.

Prior restraints carry a heavy presumption of unconstitutionality.[136] They are only permitted in "exceptional cases," one of which may be a threat to national security.[137] Although the standard for determining the sufficiency of the threat to national security is unclear, some general principles can be gleaned from the opinions submitted in *New York Times Co. v. United States*.[138] The majority of the court felt that, to sustain a prior restraint, the government has the burden of showing by clear and convincing evidence[139] that disclosure of the information would cause direct and immediate grave harm to the nation.[140] This standard reemphasized the Court's belief that prior restraints are unconstitutional except in an extremely narrow range of cases.[141] This is the standard that should be used in evaluating the constitutionality of using the ITAR to effectuate prior restraints.

2. *Prior Restraints, Cryptology, and the ITAR*

Although the Munitions Control Center has indicated that the ITAR does not and will not be interpreted by the government to im-

136. New York Times Co. v. United States, 403 U.S. 713, 714 (1971).

137. Near v. Minnesota, 283 U.S. 697, 716 (1931).

138. 403 U.S. 713 (1971).

139. *Id.* at 714.

140. *Id.* at 726-27 (Brennan, J., concurring); *id.* at 730 (Stewart and White, JJ., concurring). The dissenters in *New York Times* (Harlan and Blackmun, JJ., and Burger, C.J.) agreed that the decision was too rushed to properly determine whether the harm was sufficiently direct and immediate that the injunction should stand.

141. One of the criticisms of this test from a national security standpoint arises from the nature of modern warfare. The greater one's intelligence gathering ability, the better one is able to predict, counter, and defeat one's enemy. The ability to decipher intercepted messages gives a nation an advantage over its enemy in times of war. The Battle of Britain is an example of this. The pilots for the Allied Forces approached out of the sun when attacking the waves of bombers from Germany. The knowledge of when and where the bombers would attack came from deciphering secret codes.

Disclosure of the United States Code today may not harm the government immediately. The result in the future could be devastating. The *New York Times*' test is an attempt to balance the potential danger against the value Americans place on free speech. The potential effects of disclosing information vital to national security almost always will outweigh a single case of censorship. The *New York Times*' test and the general presumption against prior restraints rest on the realization that it would be difficult to argue for freedom of speech in an individual instance. For an excellent application and discussion of this position see Cheh, *The Progressive Case and the Atomic Energy Act: Waking to the Dangers of Government Information Controls*, 48 GEO. WASH. L. REV. 163, 197-202 (1980).

pose a prior restraint on publication,[142] that is not the end of the prior restraint issue. In the present system, researchers in basic mathematics submit to a voluntary review, prior to publication, by a committee of peers and interested government officials. This provides an opportunity for the government to effectuate a prior restraint.[143] The government knows of the research prior to its publication and, based on statutory authority, can ask the scientist and publisher to refrain from publishing the article. If the scientist does not agree, the government may seek an injunction.[144] If the scientist publishes the article in violation of the injunction, he will be in contempt of court and, as in *Walker v. City of Birmingham*,[145] unable to raise appropriate constitutional claims.

Given the *New York Times'* test for prior restraints in national security contexts, however, and the likelihood that development of sophisticated cryptologic devices will not cause *immediate* harm, a prior restraint would be unjustified and unconstitutional if used to restrict publication of research.

A tougher case is presented if the research reveals a government code.[146] The government may be able to sustain the burden of showing a "direct and immediate grave harm," thereby justifying a prior restraint. The government should, however, be required to

142. *See supra* note 88 and accompanying text.

143. *See* J. NOWAK, R. ROTUNDA, & J. YOUNG, *supra* note 114, at 741-45. A criminal action would result in subsequent punishment. To pursue a criminal penalty, the state must proceed through the complex procedures associated with a jury trial. If the state loses its case, it cannot appeal because of the double jeopardy clause of the Fifth Amendment.

A civil injunction enjoining the illegal activity avoids some of the procedural complexities. It is an equitable remedy and will be heard before a judge, not a jury. A temporary restraining order may be issued quickly, with the hearing held at the earliest possible date thereafter. Because it is a civil case, the standard of proof is lower than in a criminal trial, and the government has a right to appeal the ruling. An injunction is a court order, and violation of it results in contempt of court, regardless of the merits of the claim. Since violation of the Arms Export Control Act or its regulations subjects the offender to a fine, imprisonment, or both, 22 U.S.C. § 2778(c) (1982), an injunction could be used to prevent publication of cryptology research, pending resolution of a claim that the restrictions of the ITAR on publication of basic research in cryptology are unconstitutional. It is ironic that a prior restraint could be used to restrict publication pending resolution of the constitutional issues, one of which is a claim of impermissible prior restraint.

144. A similar situation arose in United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979). For an insightful discussion of the case, the Atomic Energy Act, and the constitutional issues raised, see Cheh, *supra* note 141.

145. 388 U.S. 307 (1967).

146. In this case, the espionage statute may also be brought in as the basis for an injunction. *See supra* notes 96-102 and accompanying text.

make that showing.[147]

The constitutionality of prior restraints depends upon the level and immediacy of the potential harm. The government will only succeed if national security is threatened with immediate grave harm. Given the past claims of national security risks, courts are liable to view the government's claim with some skepticism and hold the government to the standard in *New York Times*, an onerous burden at best. Like overbreadth analysis, prior restraint analysis is more favorable to publication than NSA would like.

C. Time, Place, and Manner Restrictions

In *Elder Industries*, the court concluded that 22 U.S.C. § 1934 controlled conduct rather than restrained speech.[148] As interpreted by the Supreme Court, the First Amendment allows the government to place reasonable time, place, and manner restrictions on conduct while pursuing its legitimate objectives, "even though incidental limitations upon expression may result."[149] In *Elder Industries*, the court properly noted that, whenever a government regulation impinges on freedom of speech, its scope must be narrowly drawn. By limiting the applicability of the ITAR to exports of technical data "significantly and directly related to specific articles on the Munitions List,"[150] the court was able to narrow the statute so that it was constitutional under the time, place, and manner standards enunciated by the Supreme Court.

Since that decision, there have been at least three cases[151] that have, to some extent, changed the tests the Court applies in this area.

In *Schad v. Mt. Ephraim*[152] and *Heffron v. International Society for Krishna Consciousness*,[153] the Court identifies five elements that validate enactment of a time, place, and manner restriction. First, the regulation must not be based on the content or subject matter of

147. Separating cryptology research revealing government codes from research that allows development of cryptologic devices is meant to indicate that courts may balance the weight of these harms differently under prior restraint analysis. This Note suggests that revealing a government code is more drastic than developing sophisticated cryptology devices that limit NSA's signal intelligence activities.

148. 579 F.2d at 521.

149. *Id.* at 520.

150. *Id.*

151. Schad v. Mt. Ephraim, 452 U.S. 61 (1981); Heffron v. Int'l Soc. for Krishna Consciousness, 452 U.S. 640 (1981); Metromedia, Inc. v. City of San Diego, 453 U.S. 490 (1981).

152. 452 U.S. 61 (1981).

153. 452 U.S. 640 (1981).

the speech.[154] Second, it must not be subject to arbitrary application.[155] Third, the regulation must serve a significant governmental interest.[156] Fourth, there must not be a less restrictive alternative available.[157] Finally, there must be adequate alternative channels of communication.[158] The zoning power involved in these cases is similar to the federal government's ability to regulate arms exports. It is a fundamental responsibility of that segment of government.

Applying these tests to the ITAR's restrictions on cryptology research is inconclusive. The ITAR attempts to regulate transfers of defense articles and defense services. Normally, this regulation would be construed not to be based on content or subject matter, since it does not address any particular speech; thus it would meet the first test on its face. If basic scientific research in cryptology qualifies as technical data, however, the ITAR regulates the ability of the researcher to publish, and publishing is a traditional element of speech.

The regulations appear to pass the arbitrariness requirement. Normal procedure under the ITAR requires that a specific reason be given for denial of a license; procedures for appeal of that ruling exist.[159]

The regulations do serve national security and foreign policy interests of the government. These interests are obviously significant. In *Elder Industries*, the court noted that restrictions were imposed on a commercial concern and, although commercial speech is protected by the First Amendment, it is not protected to the same degree as political speech.[160] Although these governmental interests may have been significant in comparison to commercial speech, when compared with nongovernmental cryptology research, a different balance to the equation may result. The government's interest is greater, but the significance of the researcher's speech has also increased. It is not commercial speech, but the fundamental speech activity of publishing that is being abridged. This may offset na-

154. *Heffron*, 452 U.S. at 648.

155. *Id.* at 649.

156. *Id.*

157. *Id.* at 654.

158. *Schad*, 452 U.S. at 75-76.

159. According to the court in *Elder Industries*, 579 F.2d at 522 n.2, Elder Industries could have sought administrative review of the initial license denial under 22 C.F.R. § 123.05(c) (1977), or a hardship exception under 22 C.F.R. § 126.10 (1977). In addition it could have sought judicial review of that decision under the Administrative Procedure Act, 5 U.S.C. § 702 (1976).

160. *Elder Indus.*, 579 F.2d at 519-20.

tional security as a persuasive governmental interest in satisfying the third part of this five part test.

Given the goal of national security, licensing seems to be the best way to achieve it. Thus, the less restrictive alternative requirement is met. The fifth requirement of adequate alternative channels of communication may be inapplicable when the goal of the restriction is to deny any export of communication.

Heffron implies that at least the first four tests must be met for the regulation to be a valid time, place, and manner restriction.[161] Given the inconclusiveness of these tests, it is unclear how the court would rule in applying them to restrictions imposed on publication of nongovernmental research in cryptology. In any event, the inconclusiveness of the time, place, and manner restrictions, coupled with the strong arguments for invalidating government restrictions on cryptology research in overbreadth and prior restraint analysis, suggests that NSA can not constitutionally impose the restrictions of the ITAR on nongovernmental research.

V. CONCLUSION

NSA heralded the decision in *Elder Industries* as support for its position on cryptology research. The director, however, has indicated a need for more authority.[162] NSA, implicitly at least, has realized that it cannot legally control nongovernmental cryptology research or its publication. This Note emphasizes that lack of legal control. What then, are the options available to NSA?

If NSA is correct, slowing down the development of nongovernmental codes will keep NSA in the forefront of cryptology, at least in the United States. The voluntary prior restraint system in which the nongovernmental research sector is participating is effective in inhibiting private development of cryptologic devices. The forewarning given the government allows appropriate legal action to be taken if warranted. The dialogue itself also provides an opportunity to inhibit development and dissemination without resorting to the courts.[163]

Nevertheless, that is probably not the answer. The business community also needs security. If it is not available, the consequences could be just as devastating as the inability of the United

161. *Heffron*, 452 U.S. at 648-55.

162. Inman, *supra* note 6, at 134; Shaply, *supra* note 56. The past director of NSA, Admiral Inman, would like NSA to have power equivalent to that of the Atomic Energy Commission—the power to render classified any cryptology work that would jeopardize national security.

163. Wallich, *supra* note 63.

States to cryptanalyze data from Third World countries.[164] Development must proceed. The loss of signal intelligence due to the availability of better cryptologic devices on the market is probably no greater than the gain in security for private business. This may not be true of developments that break government codes. Showing that the code can be broken, however, should be an adequate warning that the government needs to change its codes.

In either case, when freedom of speech is added, there is little room to argue that restricting nongovernmental research is constitutional. The constitutional doctrines of overbreadth and prior restraint, as applied by the Supreme Court, will prevent the government from restricting and controlling dissemination of this type of research.

This is proper. Publication should be allowed unless the potential harm is so great that, if the cryptology information is published, it will "immediately and directly" harm the national interest. The right to free speech cannot be abridged on the basis of "surmise or conjecture that untoward consequences may result."[165]

In the final analysis, national security risks and a loss of First Amendment freedom may result from undue governmental restraint of cryptologic developments. Accordingly, a congressional committee comment referring to the Atomic Energy Act is equally applicable to NSA's desires to inhibit cryptology research: "However well intentioned, however loosely or intelligently enforced, such action is a latent danger to the life of this democracy."[166]

Christy Brad Escobar

164. Kahn, *supra* note 14, at 22, 26.
165. *New York Times*, 403 U.S. at 725-26.
166. H.R. REP. NO. 1758, 85th Cong., 2d Sess. 18 (1958).