Preface

In January of 1993 the National Institute of Standards and Technology (NIST) initiated the preparation of this and other publications on various aspects of the civilian cryptography issue. The purpose of this project was to prepare concise summaries of information, based upon research in open source literature, on a particular topic of interest relevant to the public discussion of cryptographic-related issues.

This study was prepared under contract from the National Institute of Standards and Technology (NIST).

Comments, additions, or corrections on this study are welcomed, as it is our intent to update it periodically. Submissions should be directed to:

Mr. Lynn McNulty
Associate Director for Computer Security
Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

Fax: 301-948-1784
E-mail: mcnulty@ecf.ncsl.nist.gov

Thank you.

REVIEW AND ANALYSIS OF U.S. LAWS, REGULATIONS, AND CASE LAWS PERTAINING TO THE USE OF COMMERCIAL ENCRYPTION PRODUCTS FOR VOICE AND DATA COMMUNICATIONS

Professor James P. Chandler
Diana C. Arrington
Donna R. Berkelhammer
William L. Gill

January 1994

Prepared by
National Intellectual Property Law Institute and
The George Washington University
1350 Eye Street NW, Suite 820
Washington, DC 20005
Subcontract No. 19K-RF105C

DOE Project No. 2042-E024-A1

Prepared for
Data Systems Research and Development Program
Technical Operations
Oak Ridge K-25 Site
Oak Ridge, Tennessee 37831-7620
Managed by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-84OR21400

K/DSRD/SUB/93-RF105/2
Limited Distribution

REVIEW AND ANALYSIS OF U.S. LAWS, REGULATIONS, AND CASE LAWS
PERTAINING TO THE USE OF COMMERCIAL ENCRYPTION
PRODUCTS FOR VOICE AND DATA COMMUNICATIONS

Professor James P. Chandler
Diana C. Arrington
Donna R. Berkelhammer
William L. Gill

January 1994

Prepared by
National Intellectual Property Law Institute and
The George Washington University
1350 Eye Street NW, Suite 820
Washington, DC 20005
Subcontract No. 19K-RF105C

DOE Project No. 2042-E024-A1

Prepared for
Data Systems Research and Development Program
Technical Operations
Oak Ridge K-25 Site
Oak Ridge, Tennessee 37831-7620
Managed by
Martin Marietta Energy Systems, Inc.
for the
U.S. Department of Energy
under contract DE-AC0584OR21400

CONTENTS

EXECUTIVE SUMMARY

This document analyzes issues pertaining to the use and regulation of encryption technology. Section 1 of this document analyzes constitutional issues pertaining to encryption technology. The first issue deals with the freedom of speech and the First Amendment and addresses whether encrypted speech is protected speech, whether requiring encryption key disclosure to the government violates a user's freedom of speech, whether a government's prohibition against use of certain cryptographic technologies infringes upon freedom of speech, and whether governmental control of encryption technology through export and import laws infringes an individual's freedom of speech. Next, the right to privacy and the First Amendment is analyzed, addressing whether government prohibition against use of certain cryptographic technologies infringes an individual's right to privacy and whether a key escrow system that allows access to encrypted speech infringes right to privacy.

The analysis of the Fourth Amendment deals with the issue of illegal search and seizure of stored and voice communications. Pertaining to stored communications, this section addresses whether the government can seize encrypted electronic/computer stored documents without prior notification to owner, and whether requiring disclosure of an encryption key to the government in advance of probable cause to seize communications is violative of the Fourth Amendment. With respect to voice and data transmission, the issues of whether, in a situation where one or both users of the proposed key escrow system are located outside the borders of the United States, a warrant requirement exists to seize voice or data communications, whether the government can seize encrypted electronic/ computer communications without prior notification to owner, and whether requiring disclosure of an encryption key to the government in advance of probable cause to seize voice and data communications is violative of the Fourth Amendment.

Analysis of the Fifth Amendment addresses the key escrow system and the privilege against compelled self-incrimination. The key issue is whether a key escrow system that may involuntarily secure from the user the “key” to decipher the user's encrypted messages violates the Fifth Amendment's privilege against self-incrimination.

Section 2 of this document analyzes the current state of the law pertaining to the statutes and rules regulating the domestic use, exportation, and importation of encryption technology. With respect to the control of the export of encryption technology, an overview of the Arms Export Control Act, the Export Administration Act, and the Invention Secrecy Act is given, and their relation to

encryption technology is summarized. For import controls, an overview of controls of permanent and temporary imports by the State Department, the Treasury Department, and the Federal Communications Commission is given, and the impact on the importation of encryption technology is summarized.

ABSTRACT

This document analyzes issues pertaining to the use and regulation of encryption technology. Section 1 covers constitutional issues pertaining to encryption technology. The first issue deals with the freedom of speech and the First Amendment and addresses whether encrypted speech is protected speech, whether requiring encryption key disclosure to the government violates a user's freedom of speech, whether a government's prohibition against use of certain cryptographic technologies infringes upon freedom of speech, and whether governmental control of encryption technology through export and import laws infringes an individual's freedom of speech. Next, the right to privacy and the First Amendment is analyzed, addressing whether government prohibition against use of certain cryptographic technologies infringes an individual's right to privacy and whether a key escrow system that allows access to encrypted speech infringes right to privacy. Analysis of the Fourth Amendment deals with the issue of illegal search and seizure of stored and voice communications. Analysis of the Fifth Amendment addresses the key escrow system and the privilege against compelled self-incrimination. Section 2 of this document analyzes the current state of the law pertaining to the statutes and rules regulating the domestic use, exportation, and importation of encryption technology.

ACRONYMS

ADPTEautomated data processing and telecommunications equipment
AECAArms Export Control Act
CCLCommerce Control List
CIACentral Intelligence Agency
DESData Encryption Standard
EAAExport Administration Act
EARsExport Administration Regulations
ECPAElectronic Communications Privacy Act
FCCFederal Communications Commission
FISCForeign Intelligence Surveillance Court
ISAInvention Secrecy Act
ITARInternational Traffic in Arms Regulations
NISTNational Institute of Standards and Technology
NSANational Security Agency

1. CONSTITUTIONAL ISSUES REGARDING USE

1.1 FIRST AMENDMENT

1.1.1 Freedom of Speech

1.1.1.1 General issues

1.Is encrypted speech protected speech under the First Amendment?

2.Does requiring encryption key disclosure to the government in a particular technology violate the user's right to freedom of speech under the First Amendment?

3.Does a government prohibition against use of certain cryptographic technologies infringe an individual's right to freedom of speech under the First Amendment?

4.Does governmental control of certain cryptographic technologies through export/import laws infringe an individual's right to freedom of speech under the First Amendment?

1.1.1.2 State of the law

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press, or the right of people peaceably to assemble, and to petition the government for a redress of grievance."[1] Currently, it appears that the Supreme Court is advancing toward a hierarchical view of the First Amendment, which assigns different levels of constitutional protection to different kinds of expression. The Court considers "protected speech" speech that the First Amendment protects against prior restraints and punishment after the fact.[2] Because all speech is not protected to the same degree, protected speech falls into two categories, "fully protected speech" and "middle-tier speech." Fully protected speech is speech protected to the limits of the First Amendment's scope as defined by the Supreme Court.[3] The Court has stated that speech of "literary, political, or scientific value" is more likely to be protected.[4] In *Ohralik v. Ohio State Bar Association*, the Court held that commercial speech deserves only a "limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values."[5] The distinction between fully protected speech and middle-tier speech (i.e., commercial speech) appears when the government attempts to suppress speech content.[6] If the government attempts to control

---

1.U.S. CONST. amend. I.

2.Funk, Roger, *National Security Controls on the Dissemination of Privately Generated Scientific Information*, 30 UCLA L. Rev. 405, n.209 (1982).

3.*Id.* at 435. Several kinds of speech are not afforded First Amendment protection, such as perjury, blackmail, fighting words, defamation, obscenity, fraud, and commercially deceptive advertisements.

4.*FCC v. Pacifica Foundation*, 438 U.S. 726, 746 (1978).

5.436 U.S. 447, 456 (1978); the Court first suggested that commercial speech would not receive full protection in *Virginia State Board Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748, 771 (1976).

6.Funk, *supra*, at 437-38.

communicative speech in order to suppress a viewpoint or because it fears what the message will prompt or enable the audience to do, the government must demonstrate a "compelling" interest in the case of fully protected speech[7] and "substantial" interest for middle-tier speech.[8] Alternatively, if the government tries to regulate only the noncommunicative impact of protected speech, regulation is allowed so long as it does not unreasonably interfere with the speaker's communication of their message to the targeted audience or leaves other alternative means for communication.[9] In the case of both tiers of speech, the regulatory methods must precisely serve the asserted governmental interest, and they must be the least restrictive of all means available to the government.[10]

The Supreme Court has not decided whether the use of cryptography, encrypted speech specifically or scientific speech is protected under the First Amendment.[11] The Court in *Virginia Pharmacy* held that commercial speech is not subject to complete suppression by the state, and it considered three major interests that lie at the heart of the freedom of speech guarantee: (1) the individual interests of the giver and receiver, (2) societal interest in the free flow of information, and (3) societal interest in enlightened decision making.[12] Communication of scientific and technological information serves the first interest of individual self-expression because scientific expression is largely an individualistic and creative process.[13] These interests are intellectual in nature, and thus, unlike commercial advertising, they are fully consistent with the general views of free expression and self-realization.[14] The second interest is served because the free flow of scientific information allows the scientist to draw on the work and experimentation of colleagues, which guards against scientific error, therefore promoting discovery of scientific truth and fostering technological advancement.[15] Finally, scientific expression is essential to informed public decision making for a wide range of the major policy issues, from environmental concerns to foreign policy.[16] Accordingly, the Supreme Court could very likely afford scientific speech full protection under the First Amendment.[17]

Commercial speech. The Court defines "commercial speech" as that proposing a commercial transaction,[18] rather than using an earlier and broader definition of commercial speech "related solely to the economic interests of the speaker and its audience."[19] However, most scientific speech

---

[7]. *First Nat'l Bank v. Bellotti*, 435 U.S. 765, 786 (1978) (when a prohibition is directed toward speech content and the speech is intimately related to the government, the subordinating interest must be compelling, that is, of the highest order of such interests).

[8]. Funk, *supra*, at 437; see *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 564 (1980) (when commercial speech is neither misleading nor related to unlawful activity, the subordinating interest must be "substantial").

[9]. Funk, *supra*, at 438; see *Consolidated Edison Co. v. Public Serv. Comm'n*, 447 U.S. 530, 535 (1980), "time, place, or manner" regulations intended to control noncommunicative effects of speech are permitted if they "serve a significant governmental interest and leave ample alternative channels for communication." "The essence of time, place, or manner regulations lie in the recognition that various methods of speech, regardless of their content, may frustrate legitimate governmental interests." *Id.* at 536.

[10]. Funk, *supra*, at 438.

[11]. Generally, scholarly authorities, who have written on this topic, consider scientific speech or information to include both scientific principles ("basic" science) and their technological applications ("applied" science). Funk, *supra*, at 406 (1982). See, generally, Shinn, Allen, Jr., *The First Amendment and the Export Laws: Free Speech on the Scientific and Technical Matters*, 58 Geo. Wash. L. Rev., 368 (1990); Ferguson, James R., *Scientific Inquiry and the First Amendment*, 64 Cornell L. Rev. 639 (1979).

is concerned with the advancement of knowledge, which serves an interest well beyond narrow economic concerns and proposes more than just a commercial transaction. Thus, the Court would likely classify scientific speech as noncommercial.[20] The sole context in which commercial speech cases have been heard before the Supreme Court has dealt with advertising, which has motivated the Justice Department to conclude that technical data would not be commercial speech merely because these data were available for a fee.[21] Even though private communication of proprietary technological information often serves commercial purposes, commercial value is usually the reason for maintaining its proprietary status.

All noncommercial speech, however, is not entitled to full First Amendment protection. The Court has clearly stated that "matters of public concern [are] at the heart of the [F]irst [A]mendment's protection."[22] Beyond this area, the Court has tried to balance the interests of the state in regulating societal evils against interest in public communications. Therefore, if scientific speech speaks to matters of public concern, it should receive full protection. However, if such speech is not concerned with public affairs and is regulated by export laws, the Court would presumably balance national security interests against the First Amendment.[23]

Speech incidental to regulated conduct. Speech that is incidental to regulated conduct may receive no First Amendment protection at all. Currently, the government does control exports of particular articles; therefore, it can control speech to the extent necessary to make control of the articles effective.[24] In *Ohralik v. Ohio*, the Supreme Court concluded that it has never been deemed an "abridgement of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed."[25] The *Ohralik* court cited antitrust, securities regulations, and labor relations as areas of governmental-regulated conduct despite a large component of written or spoken speech.[26] The relation between speech and properly regulated conduct was the rationale behind the Court's decision in *United States v. Edler*.[27] In this case, the defendant was convicted of exporting technical data which outlined a process for making missile cases without a license under the U.S. Munitions List.

---

12. *Virginia Pharmacy*, 425 U.S. at 761-65.

13. Shinn, *supra*, at 378.

14. Ferguson, *supra*, at 647.

15. Id.

16. Shinn, *supra*, at 378-79.

17. *Id.* at 379; see Allen, *supra*, at 436.; see also Ferguson, *supra*, at 649.

18. *Virginia Pharmacy*, 425 U.S. at 762.

19. *Central Hudson*, 447 U.S. at 561.

20. Shinn, *supra*, at 379.

21. *Id.* 379; see Office of Legal Counsel, Department of Justice, Memorandum for William B. Robinson, Office of Munitions Control, Department of State 12 (July 1, 1981).

22. *Nat'l Bank*, 435 U.S. at 776; See, *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 758 (1985).

23. Shinn, *supra*, at 380.

24. *U.S. v. Edler Industries*, 579 F.2d 516 (9th Cir. 1978).

25. 436 U.S. 447, 456 (1978).

26. *Id.*

x
The Court held that the federal government definitely possesses the authority to regulate the international arms traffic, and, as a necessary incident to that authority to control arms export, the President has authority to control the flow of information concerning the production and use of arms.[28] The *Edler* court held that the U.S. Munitions List was not overbroad, by restricting the definition of "technical data" to include data that are "significantly and directly related" to specific articles on the Munitions List.[29] While restricting the definition of technical data, the Court cited First Amendment concerns if the definition were to be broader.[30] The Justice Department after reviewing *Edler* applied the same rationale to the Export Administration Regulations (EARs) and concluded that the far greater range of information and technology sought to be regulated by the EARs made it unlikely that these regulations could meet the restraints imposed by *Edler*: "It is apparent that the [EARs] apply a prior restraint in the form of a licensing requirement, to a wide variety of protected speech."[31]

Prior Restraints. The doctrine of prior restraint applies to fully protected speech. A prior restraint attempts to prevent an act of communication from occurring.[32] Any system of prior restraints is adjudicated by the Supreme Court, bearing a heavy burden of showing justification for the imposition of such a restraint.[33] Prior restraints are allowed when subsequent punishment cannot protect an extremely important governmental interest.[34] A system of prior restraint of expression comes in two forms: administrative licensing schemes and judicially imposed injunctions. In the former category is a group of cases in which the Court has rejected licensing schemes requiring executive approval prior to use of public facilities for political or religious purposes, display of motion pictures, distribution of pamphlets, and public parades and demonstrations.[35]

Licensing schemes, such as the Arms Export Control Act and the Export Administration Act, must meet strict standards to guide the licensing authorities so that constitutional standards can be met, otherwise such schemes may prohibit constitutionally protected speech. Thus, licensing schemes tend to restrain speech that is protected but that is close to the definition of unprotected speech.[36] The leading case which involves prior restraint of judicial injunctions is *Near v. Minnesota ex rel. Olson*, in which the defendant had published a series of articles critical of several public officials in violation of a Minneapolis statute that granted judicial abatement of any newspaper deemed "malicious, scandalous, and defamatory."[37] The district court granted an injunction sought by the officials to shut the newspaper down. The Supreme Court reversed, concluding that such a statute was the "essence of censorship."[38] *Near* established the doctrine of judicial injunctions as a form

---

27. *Edler*, 579 F.2d at 518.

28. *Id.* at 520; see *U.S. v. Posey*, 864 F.2d 1487, 1469 (9th Cir. 1989).

29. *Id.* at 521.

30. *Id.* at 520.

31. Shinn, *supra*, at 381 [quoting for the Office of Legal Counsel, Department of Justice, Memorandum for Henry D. Mitman, Department of Commerce 4 (July 28, 1981)].

32. Emerson, *The Doctrine of Prior Restraint, 20 Law & Contemp. Probs.*, 648, 648 (1955); see Funk, *supra*, at 444.

33. *New York Times*, 403 U.S. at 714.

34. *Id.* at 727 (Brennan, J., concurring); Id. at 727-30 (Stewart & White, JJ., concurring).

35. Shinn, *supra*, at 382.

36. Id.

37. 283 U.S. 697 (1931).

of prior restraint.[39]

There are important distinctions between prior restraint through administrative licensing and through judicial order. In licensing schemes, an administrative official often acting ex parte and frequently without clear standards, and almost always without training to distinguish what is and is not protected, can quickly and easily prohibit speech, publication, or demonstration.[40] The applicant has the burden to seek judicial review. In contrast, when the government seeks to prohibit speech through judicial injunction, it carries the heavy burden. The government must sue in open court and persuade an impartial and trained judge to issue such an order. With administrative licensing, the risk that protected speech will actually be prevented is great; with injunction, the risk is slight. Therefore, the important differences between them can be blurred when both are simply referenced as prior restraint.[41]

National Security Exception. Executive Order 12356 defines national security as the “national defense or foreign relations of the United States.”[42] The Constitution Preamble gives “national defense equal status with the blessings of liberty.”[43] The Supreme Court in *Haig v. Agee* recognized that national security is the most important interest that could be threatened by uncontrolled dissemination of speech.[44] Nevertheless, in *New York Times Co. v. United States*, Justice Harlan in dissent stated that constitutional considerations forbid a “complete abandonment of judicial control” of the President's authority to determine issues that threaten national security.[45]

Assuming scientific information is protected speech, it would still be necessary to determine the nature of that speech whose dissemination could pose either a “compelling” or “substantial” threat to national security.[46] In the case of fully protected speech, a “compelling” threat to national security is a danger that poses an immediate,[47] certain,[48] and exceptional[49] threat. For instance, fully protected scientific information is subject to regulation if it conveys a message that would allow a potential or actual enemy to develop a significant weapon or countermeasure to a U.S. weapon within a period too short for the United States to take corrective measures.[50] For example, an immediate threat would entail a short time frame from receipt of an article by a foreign power to its actual application, as measured on an appropriate time scale of technological development.[51] A

38. *Id.* at 702.

39. Shinn, *supra*, at 383.

40. *Id.* at 384.

41. Id.

42. Exec. Order No. 12356, 3 C.F.R. 166 (1983), reprinted in 50 U.S.C. 401 at 51-6 (1982).

43. Fein, Bruce E., *National Security and the First Amendment: Article: Access to Classified Information: Constitutional and Statutory Dimensions*, 26 Wm & Mary L. Rev. 805, 806 (1985); see U.S. CONST. Preamble.

44. 453 U.S. 280, 306-08 (1981); see Funk, *supra*, at 439.

45. 403 U.S. 713, 757 (1971) (Harlan J. dissenting) [quoting *U.S. v. Reynolds*, 345 U.S. 1, 8 (1953)].

46. Funk, *supra*, at 439.

47. *New York*, 403 U.S. at 726-27.

48. *Id.*

49. *Near*, 283 U.S. 716.

50. 30 UCLA Law Rev. at 440, n.239.

certain threat is created if the information poses a threat with direct military application or related production applicability.[52] Scientific information poses an exceptional threat when it would give the enemy an "identifiable military advantage over the United States in military terms."[53]

In determining whether scientific information poses a substantial threat, the above three criteria are applicable.[54] If the possible time of application is remote as measured on an appropriate time scale of technological development, the threat to national security is too speculative to justify controls.[55] Accordingly, if the information has uncertain military or related application, again the threat may be too speculative.[56] If the United States is not the exclusive source, attempts to control the information would seem to serve no "rational purpose."[57]

In national security cases, many courts and commentators have often suggested that there is an exception to the prior restraint doctrine.[58] These cases suggest that if there is such an exception, it allows the government only to seek an injunction in appropriate situations, not the use of an administrative licensing procedure.[59]

The judicial recognition of the national security exception stems from *Near*,[60] in which the Court stated that although the defendant's conduct would not justify an injunction, there might be circumstances involving national security that would provide justification for one. The Court in *Near* applied a "clear and present danger" test,[61] which has evolved into a more speech-protective test articulated in *Brandenburg v. Ohio*.[62] The national security exception was implicitly affirmed when the government sought to enjoin the Pentagon Papers in *New York Times, Inc. v. United States*, when the district court denied the government's motion for an injunction. However, the Second Circuit Court issued a stay and remanded, relying on the exception. The Supreme Court finally reversed and held that the government did not carry its burden. In concurrence, Justice Stewart argued that an injunction would be improper because the publication would not "surely result in direct, immediate, and irreparable damage to our nation or its people."[63]

---

51. Id.

52. Id.

53. Id.

54. *Id.* at 440-41.

55. *Id.* at 441.

56. Id.

57. Id.

58. Shinn, *supra*, at 384; see *U.S. v. Donas-Botto*, 363 F.Supp. 191, 1194 (E.D. Mich. 1973). This case involved the export of blueprints and technical data concerning an armored vehicle. The district court disposed of the First Amendment: 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; *U.S. v. Van Hee*, 531 F.2d 352 (6th Cir. 1976) (First Amendment was not raised on appeal); Department of Justice, Constitutionality Under the First Amendment of ITAR Restrictions on Public Cryptography 4 n.7, reprinted in the Government Classification of Private Ideas: Hearings Before a Subcomm. of the House Comm. on Government Operations, 96th Cong., 2d Sess. 268 (1980).

59. 58 Geo Wash. Law Rev. at n.108.

60. 283 U.S. 697 (1931).

These decisions might suggest that the government could not carry its burden unless the information involved was classified and would have a difficult case to make even if classified.[64] The Pentagon Papers were classified, and the examples suggested in *Near*?"the sailing dates of transports or the location of troops?might also be expected to be classified."[65] These cases reveal that there is a narrow national security exception to the prior restraint doctrine but that it is limited to cases involving classified information. Even then the government has the burden to show in seeking an injunction that release of the information would cause immediate and serious damage to the national interest.[66]

1.1.1.3 General issues addressed

First general issue. In the first general issue?Is encrypted speech protected speech under the First Amendment??the Supreme Court has not decided whether the use of cryptography, encrypted speech specifically or scientific speech is protected under the First Amendment.[67] The Court in *Virginia Pharmacy* considered three major interests that lie at the heart of the freedom of speech guarantee. In an analysis of these interests, the Supreme Court could very likely afford these forms of speech full protection under the First Amendment.[68] However, encrypted speech and the use of cryptography are not essential to public debate on major issues of the day. Indeed, it could be argued that the use of encrypted speech inhibits full and free debate.

Several commentaries have explored First Amendment protection in the preservation of the "electronic forum, which impacts the use of cryptographic technology."[69] The electronic forum encompasses the electronic media (i.e., radio, television, cable satellite, bulletin boards, voicemail, facsimile), and information systems (computer or electronic hardware, software, human users, data).[70] The direction of recent First Amendment jurisprudence has displayed that the nature of the forum in which expression occurs tends to define the scope of protection for that forum.[71] Therefore, the nature of the electronic forum will become the main issue of an inquiry into the First Amendment rights for electronic or computer-based expression. As forms of communication proliferate, and as problems that are unique to a particular technology or format are discovered, further fragmentation of the First Amendment doctrine will occur.[72] While a few general principles may still apply to all media, differences in treatment among media can be expected to grow.[73]

---

61. *Id.* at 716.

62. 395 U.S. 444 (1969) (per curiam).

63. *New York Times*, 403 U.S. at 730.

64. Shinn, *supra*, at 385.

65. *Near*, 283 U.S. at 716; *United States v. The Progressive*, 467 F.Supp. 990 (dismissed 610 F.2d 819, 7th Cir. 1979). The district court allowed the government a preliminary injunction against publication of information that described how to construct a hydrogen bomb. Even though the defendant obtained information from the public domain, there was evidence to support that classification was appropriate.

66. Shinn, *supra*, at 387.

67. Generally, scholarly authorities who have written on this topic consider scientific speech or information to include both scientific principles ("basic" science) and their technological applications ("applied" science). Funk, *supra*, at 406. See, generally, Shinn, *supra*, at 368; Ferguson, *supra*, at 639.

68. Shinn, *supra*, at 368; Funk, *supra*, at 436.; Ferguson, *supra*, at 649. See above State of Law discussion, *supra*, at 2.

Increasingly more apparent are the difficulties in enforcing restrictions on communication in an electronic forum.[74] It is anticipated that cases will take into account the "effective limits of the law," and decisions will "implicitly reflect assumptions about media capabilities for accessing, processing, or sending information."[75] The production of information, processing of information, and transmission or publication of information are the most vulnerable areas in the communication environment.[76]

An area significant to cryptographic technology is the transmission of information. One of the most "obvious victim[s]" of the qualities of the new media will be the prior restraint doctrine, which is a means of government control that is "doomed to a condition of almost complete nonviability."[77] The two forms of prior restraints, licensing schemes and injunctions, are even more vulnerable as copying and distribution capabilities are enhanced between parties inside and outside the U.S. borders.[78] As the flow of information accelerates, it is appropriate to be mindful of a comment by a former director of the U.S. Information Agency, who stated that "the only way to censor an electronic network moving 648 million bits per second is to pull the plug."[79] While the prior restraint doctrine may be a potential casualty, the ability of punishment after the fact will also suffer. A concern definitely arises in international communications where punishment of sources located outside the U.S. borders is generally not possible.[80]

Second general issue. In the second general issue?Does requiring encryption key disclosure to the government in a particular technology violate the user's right to freedom of speech under the First Amendment??requiring disclosure of a cryptographic key, while using a government algorithm, regulates only the noncommunicative impact form of speech. Regulation of the noncommunicative impact of protected speech is allowed as long as it does not unreasonably interfere with the speaker's communication of his or her message to the targeted audience or as long as it leaves other alternative means for communication.[81] The regulatory schemes must precisely serve the asserted governmental interest and must be the least restrictive of all means available to the government.[82]

Thus, in a key escrow system, as long as the asserted governmental interest is served, the requirement

---

69. Taviss, *Dueling Forums: The Public Forum Doctrine's Failure to Protect the Electronic Forum*, 60 U. Cin. L. Rev. 757 (1992); Katsh, *The First Amendment and Technological Change: The New Media Have a Message*, 57 Geo. Wash. L. Rev. 1459, 1483 (1989).

70. Taviss, *supra*, at 758-62.

71. *Id.* at 762; Katsh, *supra*, at 1483; *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 386 (1969) ("differences in the characteristics of new media justify differences in the First Amendment standards applied to them").

72. Katsh, *supra*, at 1483.

73. Id.

74. *Id.* at 1484.

75. Id.

76. For a full discussion see *Id.* at 1485-92.

77. *Id.* at 1490.

78. Id.

79. *Id.* at 1491.

80. Id.

of the disclosure of the cryptographic keys might be permissible. A growing governmental interest within the law enforcement community is the future widespread use of commercial cryptographic technology in criminal activity and the subsequent negative implications that creates in the electronic surveillance area. Also, the government must establish that the key escrow system is the least restrictive means to protect its asserted interest. Therefore, other schemes that could possibly protect the asserted governmental interest must be explored.[83]

However, given the recently available information on the procedures governing key escrow technology, concerns arise on whether the government is requiring disclosure of an encrypted key prior to sufficient probable cause. On each cryptographic device, the government key escrow agents will possess a unique "identification number" and "chip" key particular to that chip. Once proper authorization has been secured by law enforcement and the type of key escrow encryption technology has been identified, this chip key can be secured by law enforcement to decrypt the contents of a communication. Therefore, a question arises regarding whether individuals are surrendering their encryption keys prior to the determination of probable cause. The system currently being proposed is analogous to a system of registration by the government so that it can maintain an ability to access the contents of stored electronic communications or perform electronic surveillance.[84]

Third general issue. In the third general issue?Does government prohibition against use of certain cryptographic technologies infringe individual's right to freedom of speech under the First Amendment??a government prohibition against the use of certain cryptographic devices would only infringe on an individual's right to freedom of speech if the Supreme Court determines encrypted speech to be a protected form of speech.[85] Currently, the Court has made no determination on this issue. See the first general issue (above) for a full discussion.

Fourth general issue. In the fourth general issue?Does governmental control of certain cryptographic technologies through export/import laws infringe individual's right to freedom of speech under the First Amendment??Congress is granted the authority to control exports of articles for national security purposes. The Constitution gives Congress the power to regulate foreign commerce and to do what is necessary to provide for a common defense.[86] This authority is

---

81. Funk, *supra*, at 438; see *Consolidated Edison Co. v. Public Serv. Comm'n*, 447 U.S. 530, 535 (1980) ("time, place, or manner" regulations intended to control noncommunicative effects of speech are permitted if they "serve a significant governmental interest and leave ample alternative channels for communication." "The essence of time, place, or manner regulations lie in the recognition that various methods of speech, regardless of their content, may frustrate legitimate governmental interests." *Id.* at 536).

82. Funk, *supra*, at 438.

83. Another method suggested has been fair public-key cryptography. This method differs from a key escrow system in that users voluntarily choose to register their keys, whereas in the Clipper Chip proposal the keys are registered as a component of the manufacturing process. Also the keys are associated with users; by comparison, the Clipper Chip proposal would associate the keys with the chip identification number. See Meeting of the Computer System Security and Advisory Board, June 2-4, 1993, at the National Institute of Standards and Technology, Briefing by Silvio Micali, Massachusetts Institute of Technology.

84. *Id.*

85. See Sect. 1.1.1.3, first general issue, for a full discussion.

expressed principally in three statutes: the Export Administration Act (EAA),[87] the Arms Export Control Act (AECA),[88] and the Invention Secrecy Act (ISA).[89]

Several law review articles have asserted that the EAA, the AECA, and the ISA restrict scientific and technical speech that merits constitutional protection.[90] These authorities cite (1) prior restraint without judicial review, (2) overbreadth and vagueness, and (3) regulations not narrowly tailored to a compelling state interest of national security.[91] Each of these is discussed below.

The first assertion, prior restraint through a licensing scheme, can be viewed as a lack of due process. Due process protects the liberty interests of the Fifth and Fourteenth Amendments, which include the First Amendment rights.[92] Since the landmark case of *Goldberg v. Kelly*, the Supreme Court has required some form of due process in cases in which the government has sought to deprive individuals of liberty or property interests.[93] The *Goldberg* court required New York City to provide nearly full judicial process prior to terminating welfare benefits. Other cases have firmly established this principle.[94]

The second assertion, the overbreadth doctrine, applies when fully protected speech is the object of regulation. This doctrine allows a defendant being prosecuted under a statute affecting fully protected speech to argue against it on the grounds that it restricts or "chills" the speech of others not before the court.[95] The statute must have a real and substantial impact on speech,[96] and it must be as narrowly drawn as possible.[97] Whether the export control acts would survive an overbreadth attack would presumably depend on whether the courts would regard the controlled speech as incidental to conduct.[98] In *Edler*, the AECA and International Traffic in Arms Regulations (ITAR) survived an overbreadth challenge because the court read the definition of technical data as restricted data related directly to specific articles that are subject to control and incidental to regulated conduct, thus unprotected by First Amendment.[99] As written, the ITAR is subject to an overbreadth attack; however, the judicial reaction is uncertain.[100] The EAA seems more vulnerable to overbreadth attack due to the fact the definition of technical data is much broader.[101] Although the Munitions List that

86. U.S. CONST. Preamble, art. I, § 8.

87. 50 U.S.C. §§ 2401-2420.

88. 22 U.S.C. §§ 2751-2796.

89. 35 U.S.C. §§ 181-188 (1982).

90. Shinn, *supra*, at 377; see Funk, *supra*, at 434.

91. Shinn, *supra*, at 384-94; see Funk, *supra*, at 434. The Justice expressed doubt in 1978 that the AECA provides sufficient statutory authority for the broad controls that the ITAR regulates over unclassified scientific research. The Government's Classification of Private Ideas: Hearings Before a Subcomm. of the House Comm. on Gov't Operations, 96th Cong., 2d Sess. 268 (1980).

92. *Paul v. Davis*, 424 U.S. 693, 710 (1976).

93. 397 U.S. 254 (1970).

94. Shinn, *supra*, at 389.

95. Funk, *supra*, at 441 n.249.

96. Id.

97. Funk, *supra*, at 441; *Consolidated Edison Co. v. Public Ser. Comm'n*, 447 U.S. 530, 540 (1980) (declaring that when a "government restricts the speech of a private person, the state action may be sustained only if government can show that the regulation is a precisely drawn means of serving a compelling state interest").

defines the scope of the ITAR is relatively specific, thus facilitating the holding in *Edler*, the Commodity Control List is extensive and contains a number of general catch-all entries.[102]

ISA offers the most difficult case of the three statutes. The authority to extend a secrecy order extends to any invention, in the judgment of the head of the interested government agency, that could be "detrimental to national security."[103] Neither the Act nor the regulations suggest any standard of review or guidelines by which such a judgment could be made. The lack of judicial review has the potential to restrain protected speech. Also, ISA has no regulated items or conduct to which controls on speech might be considered incidental. "ISA purports to control information itself?pure speech," a circumstance where the overbreadth doctrine is most likely to be applied.[104] However, if the Courts were to construe all information in a patent application commercial speech, the overbreadth doctrine would be inapplicable. Shinn considers this unlikely because the definition of commercial speech is that proposing a commercial transaction, and patent applications contain detailed technical descriptions of inventions, unrelated to proposing a commercial transaction.[105]

The courts have consistently upheld that the export control laws are not unconstitutionally vague.[106] The Supreme Court considers a criminal statute unconstitutionally vague if it does not provide to the defendant and the trier of fact "reasonably clear guidelines" in establishing whether a crime has been committed so as to "prevent arbitrary and discriminating enforcement."[107] Also, a vagueness challenge can be addressed only by the facts in the case before the court.[108]

In the third assertion, according to Shinn the export control regulations do not fall within the national security exception for three reasons.[109] First, the exception has been recognized only when the government sought an injunction against publication of certain information, except in the special circumstance of a Central Intelligence Agency (CIA) employee, in order to protect classified information. Thus, except for the special case of the CIA, the security exception to prior restraint amounts only to allowing the government to seek an injunction. The concern with current export control laws is that the government is not required to proceed in this manner. The possible exporter of information must apply for a license that the government can deny at will.[110] The case law makes clear that before any restraint upon protected speech may become final it must be subjected to prompt judicial review in a proceeding in which the government will bear the burden of justifying its

98. Shinn, *supra*, at 391.

99. *Edler*, 579 F.2d at 520.

100. Shinn, *supra*, at 391.

101. 15 C.F.R. § 379.1 (1988).

102. Shinn, *supra*, at n.61-63.

103. 35 U.S.C. § 181.

104. Shinn, *supra*, at 392.

105. *Id.* at 392. It would be possible for someone to include information from a patent application in such a proposal; however, the central purpose of ISA is to control all disclosure and export of controlled data, not just the use of controlled data in commercial proposals. 35 U.S.C. § 181.

106. *United States v. Gregg*, 829 F.2d. 1430 (1987); *United States v. Geissler*, 731 F.Supp. 93 (E.D. NY 1990).

107. *Smith v. Gogen*, 415 U.S. 566, 573 (1974).

108. *United States v. Geissler*, 731 F.Supp. 93 (E.D. NY 1990).

109. Shinn, *supra*, at 387.

decisions.

Second, the cases invoking national security exception have all involved or suggested a limitation to classified data. In contrast, the export laws aim primarily at unclassified data. Although the EARs do not distinguish between classified and unclassified information and the ITAR covers both classified and unclassified information, the Acts control only exports of information to foreign places, not release to American citizens. They are not necessary to control export of classified information, which is subject to much stricter regulation under executive order.[111] The national security exception is limited to protecting classified information; it cannot support export control laws concerned primarily with unclassified information.[112] The ISA extends further than the EAA or AECA, because an invention secrecy order requires that the invention be kept secret and forbids issuance of a patent. The inventor is not able to disclose the information to anyone in the United States or abroad. Therefore, the ISA imposes a kind of classification, although it does not use the term.[113]

Finally, the national security exception standard of "direct, immediate, and irreparable damage" to our nation could not conceivably be satisfied in the wide range of circumstances covered by these statutes, which regulate a full spectrum of ordinary commercial transactions.

The national security statutes clearly were not developed to regulate the noncommunicative effects of exchanges between scientists. Congress desired to control the dissemination of certain kinds of information because it feared what potential or actual enemies of the United States might accomplish with that information. It was the effect of the message on the audience, and not the means or method of communication and its interference with the achievement of an unrelated governmental purpose, that Congress intended to regulate.[114]

A recurring theme in cases implicating the First Amendment is the requirement of a close relation between the law and a compelling state interest. Therefore, a regulation that impinges on First Amendment values in order to serve a compelling state interest, but which does not in fact serve that interest, is subject to constitutional challenge. Shinn suggested three reasons why the export laws, as applied to control the flow of scientific and technical information, do not satisfy compelling state interest of national security. The main paths of leakage to other countries is espionage directed toward classified material and diversion of physical items of technology in violation of the export laws.[115] A National Academy of Sciences study found that in contrast to leakage from these sources,

110. *Edler* upheld the licensing scheme, but only because the court interpreted the definition of technical data narrowly.

111. Shinn, *supra*, at 388; Exec. Order No. 12356 (1982).

112. Id.

113. *Id.* at 392.

114. Funk, *supra*, at 439.

115. Shinn, *supra*, at 393; see National Academy of Sciences, Balancing the National Interest 71-75 (1987) (otherwise known as the Allen report). The Allen Report was chaired by General Lew Allen, former Chief of Staff of the Air Force and Director of the National Security Agency (NSA), and Bobby Iman, former Director of NSA and Deputy Director of the CIA. Despite a strong defense viewpoint, the Allen Report noted that controls should be implemented with great refrain because of the potential chilling effect on research and development. This conclusion was arrived at based on classified intelligence community briefings.

open scientific communications did not present a significant danger, mainly because of the problems of translating scientific knowledge into actual military usage.[116] Thus, if the export laws have no effect on leakage through these two most important pathways, it is difficult to see how controlling an unimportant path can serve national security interests sufficiently to justify encroaching on First Amendment rights.[117] Second, controls on scientific communications impede the progress and growth of technology, thus reducing U.S. military capabilities. The Corson Report, in examining the ways controls affect both military and economic security, stated that a policy seeking national security through scientific achievement is preferable to one based on secrecy. Third, a growing part of the world's scientific and technological capability is outside the United States, thus beyond control through export law. The Allen Report expressed this concern and determined that in many areas unilateral controls by the United States were ineffective because technology was available through other suppliers,[118] a situation very similar to the current state of encryption technology. It is hard to understand how the national interest is served by restraining communication in an attempt to control information already available elsewhere. Shinn notes that judgments about national security issues are better left to the legislatures than to the courts. Yet, when publication of information has been threatened, the courts have examined closely to see whether a sufficiently important national interest is served.

1.1.2 Privacy

1.1.2.1 General issues

1. Does a government prohibition against use of certain cryptographic technologies infringe individual's right to privacy under the First Amendment?

2. Is a key escrow system that ensures government access to encrypted speech an invasion of the right of privacy under the First Amendment?

1.1.2.2 State of the law

In a dissenting opinion, Justice Brandeis defined the constitutional right to privacy as "the right to be let alone?the most comprehensive of rights and the right most valued by men."[119] The Supreme Court has recognized freedom of association as a necessary concomitant to the specific guarantees of the First Amendment, since the exercise of freedom of speech, the press, assembly, and petition routinely requires group activity.[120] "[T]he Constitution does not provide an explicit right to privacy, and therefore its development has been slow and irregular."[121] In *Griswold v. Connecticut*, the Supreme Court declared that various guarantees in the Bill of Rights produce zones of privacy.[122]

---

116. Whether the export control acts would fail an overbreadth attack would presumably depend on whether the courts would regard the controlled speech as incidental to conduct. Scientific Communication and National Security 24-25 (1982). This first major study of the conflict between national security goals and open communication was prepared with support by the Defense Department.

117. Shinn, *supra*, at 393.

118. Allen Report, *supra*, at 54-69.

119. *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis J., dissenting).

120. Note, *The Interest in Limited Disclosure of Personal Information: A Constitutional Analysis*, 36 Vand. L. Rev. 139, 151 (1983).

Specifically, the Court recognized the zone of privacy formed by the First Amendment right of free association, the Third Amendment prohibition of peace time quartering of soldiers in homes without consent, the Fourth Amendment protection of unreasonable search and seizure of private individuals by government, and Fifth Amendment protection against self-incrimination.[123] The Constitution only protects private individuals from governmental intrusion; protection from private action is left to the states.[124] The language of the U.S. Constitution has hindered judicial development of the right to privacy; however, state constitutions have specifically recognized the right to privacy.[125]

In *Whalen v. Roe*, the Supreme Court distinguished between the "privacy of autonomy"?an "interest in independence in making certain kinds of important decisions"?and "disclosural privacy"?an "individual interest in avoiding disclosure of personal matters."[126] The right to privacy of autonomy has been recognized in decisions relating to marriage, procreation, contraception, family relationships, obscene material in the home, and child rearing and education.[127] Although the Court has continued to develop a right to privacy of autonomy, it has rarely advanced the right to disclosural privacy.[128]

Traditionally associated with the First and Fourth Amendments, disclosural privacy concerns the right of an individual to control the flow of personal information.[129] The Court has noted that freedom of association often depends on the concealment of one's associations, by the prevention of disclosure of information pertaining to a particular association.[130] The Supreme Court has seldom recognized the constitutional right of disclosural privacy,[131] and it has yet to find the right violated[132] except in a Freedom of Information Act case which weighed the public interest in disclosure against individual interest in privacy.[133]

In *Whalen*, the Supreme Court upheld a state statute requiring disclosure of private medical information to state authorities.[134] The Court emphasized the importance that the state restrictions placed on the disclosure of medical information, which made public exposure unlikely.[135] Of importance was the Court's recognition of the threat to individual privacy posed by the government collection of personal information. Justice Stevens, writing for the majority opinion declared:

---

121. Coles, Todd R., *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 Am. U. L. Rev. 957, 960; see *Paul v. Davis*, 242 U.S. 693, 712 (1976) (stating that the right to privacy is not found in any specific constitutional guarantee); *Roe v. Wade*, 410 U.S. 113,112 (1973) (finding no explicit mention of right of privacy in constitution).

122. 381 U.S. 479, 484 (1965) (recognizing right to privacy in marriage).

123. *Id.*

124. *Katz v. United States*, 389 U.S. 347, 351-53 (1967).

125. *Id.* at 964.

126. 429 U.S. 589, 599-600 (1977) (court upheld a state statute requiring disclosure of private medical information to state authorities).

127. Coles, *supra*, at 961 n.23-n.27.

128. *Id.* at n.28.

129. *NAACP v. Alabama*, 357 U.S. 449, 460-63, 466 (1958) (discussing the role of the First and Fourth Amendments and their protection to right of privacy); *Katz*, 389 U.S. at 351-53 (1967).

130. 36 Vand. L. Rev. at 151.

131. Coles, *supra*, at 962.

We are not aware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of Armed Forces and enforcement of criminal laws, all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. . . . [N]evertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, the protection of, individual's interest in privacy.[136]

While recognizing the potential threat to privacy, the *Whalen* Court refused to decide any question which might be presented by unwarranted disclosure of accumulated data, whether intentionally or by a system that did not contain comparable security standards.

Justice Brennan, in his concurring opinion, analyzed the restrictions placed on dissemination of medical data by the statute and found sufficient safeguards against unwarranted disclosure.[137] He cautioned that a constitutionally protected privacy right would be implicated if the restrictions were not in place and information was widely disseminated.[138] In a situation where a protected privacy interest was threatened, the state must establish a "compelling interest" to justify deprivation of the right to privacy.[139]

Justice Brennan, writing for the majority in *Nixon*, considered disclosural privacy involving the Presidential Records and Materials Preservation Act.[140] Under this Act, the Administrator of the General Services Administration was directed to take custody of Nixon's presidential papers and supervise their examination to determine which documents the government would keep. Reviewing the Act's screening process, Justice Brennan emphasized that the Act was written to minimize invasion of privacy and concluded that no "less restrictive means" existed to accomplish the purpose of the Act, and that Nixon's "legitimate expectation in privacy" had not been violated.[141]

While in *Whalen* and *Nixon* the Supreme Court failed to find that a constitutionally protected right to disclosural privacy had been violated, the Court has held that a similar statutorily protected privacy was violated under the Freedom of Information Act.[142] In *Reporter's Committee*, the Court found a protected privacy interest in the disclosure of personal information contained in a Federal Bureau of Investigation criminal rap sheet.[143] Balancing the public interest in disclosure against the

---

132. *Id.*; *Whalen*, 429 U.S. at 599 (finding no unconstitutional right of disclosural privacy violated); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457-59 (1977) (concluding no unconstitutional invasion of right to disclosural privacy).

133. *Department of Justice v. Reporters Comm.*, 489 U.S. 749 (1989).

134. 429 U.S. at 603-04.

135. *Id.* at 600-02.

136. *Id.* at 605-06.

137. *Id.* at 606-07.

138. Id.

139. *Id.* at 607.

140. *Nixon*, 433 U.S. at 429.

141. *Id.* at 464-65.

142. *Department of Justice v. Reporter's Committee*, 489 U.S. 749, 762 (1989).

individual interest in privacy, the Court found the former at its "nadir" and the latter at its "apex."[144] The Court concluded that disclosure of law enforcement records is an unwarranted invasion of privacy.[145]

While the Court has neither consistently recognized a disclosural privacy nor clearly outlined requirements for raising a claim of disclosural privacy, the Court seems to have determined the appropriate standard of review to be applied.[146] A heightened scrutiny test is applied, balancing individual interest in nondisclosure against government's interest in disclosure.[147]

With an explicit constitutional right to privacy in personal information held by the federal government absent, congressional legislation provided the only remaining safeguard.[148] The Privacy Act of 1974[149] was the first attempt by Congress to strike a balance between the government's interest and need to gather personal information and individuals' competing interest to keep control over personal information.[150] The Privacy Act requires every federal agency maintaining a record on an individual within a system of records to (1) allow the individual to control the use and dissemination of information contained in the record; (2) allow the individual to review, to correct, or to amend information contained in the record; (3) control and restrict the collection, use, maintenance, and dissemination of information in the record; and (4) be subject to civil suit for specified violations of the Privacy Act.[151]

The first safeguard prohibits any federal agency from disclosing any information contained in a system of records without written consent of the individual to whom the record pertains. The scope of this prohibition on nonconsensual disclosure, however, is subject to numerous exemptions. General and specific exemptions allow the heads of federal agencies to promulgate rules that exempt their federal agency's system of records from provisions of the Privacy Act.

Specific exemptions exist for law enforcement purposes in response to exigent circumstances.[152] Law enforcement officials may have access to information in a "showing of compelling circumstances affecting health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such an individual."[153]

The broadest of these exemptions, the routine use exemption, permits nonconsensual disclosure of personal information where the purpose for collection is compatible with its use by the federal

---

143. Id.

144. *Id.* at 750.

145. *Id.* at 749.

146. Coles, *supra*, at 962 n.34.

147. See Seng, *The Constitution and Informational Privacy, or How So-Called Conservatives Countenance Governmental Intrusion into a Person's Private Affairs*, 18 J. Marshall L. Rev. 871, 875 (1985).

148. Id.

149. 5 U.S.C. § 552(a) (1988).

150. Coles, *supra*, at 964.

151. 5 U.S.C. § 552a.

152. 5 U.S.C. § 552a(b)(8).

153. Id.

agency. Law enforcement agencies, such as the CIA and the Department of Justice, have employed the routine use exemption to avoid the restrictive language of an applicable disclosure exemption.[154] Neither the federal agencies nor the Office of Management and Budget have actively overseen the exemption's use, and statutory and procedural barriers have precluded the courts from averting abuse of the exemption through judicial review.[155] Because the final version of this Act was a result of a last-minute compromise between competing House and Senate bills, the Act has become an internally inconsistent statute with no reliable indication of legislative intent.

1.1.2.3 General issues addressed

First general issue. In the first general issue?Does a government prohibition against use of certain cryptographic technologies infringe individual's right to privacy under the First Amendment??given the direction of the Supreme Court's view of First Amendment privacy, this concern would either be construed as a privacy “interest in independence in making certain kinds of important decisions” (i.e., “privacy of autonomy”) or an “individual interest” in controlling the flow of personal information (i.e., “disclosural privacy).”[156] The Court continues to actively develop the right to privacy of autonomy; however, the right has only been recognized in decisions relating to family matters such as marriage, procreation, contraception, family relationships, obscene material in the home, and child rearing and education.[157] A government's attempt to regulate cryptographic use does not naturally relate to decisions involving family matters, and the Court has never decided if scientific or technological matters would be viewed in such a manner. Thus, the prohibition or regulation of certain cryptographic technologies would probably not offend the Court's current view of an individual's right in privacy of autonomy.

Although the Court has continued to develop a right to privacy of autonomy, it has rarely advanced the right to disclosural privacy.[158] In cases involving the disclosural privacy doctrine, the Court's interpretation is focused on the individual's interest in control of personal information. The prohibition of certain cryptographic technology could implicate this doctrine. However, all the cases implicating this doctrine involved instances where the local or federal government by statute had the right to disclose certain personal information. Therefore, it is not clear if the regulation of cryptography would offend a legitimate privacy right under the First Amendment.

Second general issue. In the second general issue?Is a key escrow system that ensures government access to encrypted speech an invasion of the right of privacy under the First Amendment??an encryption key escrow system where the government is the escrow agent might implicate the disclosural privacy doctrine, because it concerns the protection of an individual's interest to control the flow of personal information and the government's interest in gathering and controlling the use of personal information. The heightened scrutiny test would be applied to balance both private and government interests in disclosure of personal information. In light of the rationales used in both *Whalen* and *Nixon*, the Supreme Court would weigh the individual concerns in (1) the potential harm of disclosure of information and (2) the individual's legitimate expectation of privacy in nondisclosure, versus the government's concern in (1) the need to collect, use, or maintain individual

---

[154]. Coles, *supra*, at 980, 988.

[155]. Coles, *supra*, at 959.

[156]. Coles, *supra*, at 961 n.23-n.27.

[157]. Id.

[158]. Coles, *supra*, at 962 n.28.

information; (2) the implementation of adequate administrative procedural safeguards; and (3) the practice of the least restrictive alternative.[159]

A legitimate individual interest in the potential threat of disclosure of private cryptographic keys could have serious detrimental effects on both domestic and national security. Nonclassified data accumulated from an increasing number of sources, including hostile governments or groups, could adversely affect the national security of the United States.[160] Examples of this information are weather and crop reports, trading reports, electronic fund transfers, and various types of economic information.[161] This gives the National Security Agency (NSA) reason to be concerned with the computer security standards used by civil government agencies and private entities.[162]

The cases interpreting this doctrine considered only a privacy interest in information intimately related to that particular individual, for example, an individual's criminal record, medical information, and personal papers. A question could arise in assessing a privacy interest of an individual if the desire to use any general nonclassified cryptographic technology can give an individual a legitimate expectation of privacy. The cryptographic process is a "reversible process designed to make information unreadable to all but the intended recipient;" thus, a certain level of privacy is expected by a user.[163] Yet, the legitimate expectation of privacy centers around the encrypted data, not on the type of cryptographic technology used. Therefore, a Court must resolve the scope of a legitimate expectation of privacy on encrypted communications, which would probably be influenced to a certain extent by the type of medium used to communicate.

A governmental interest within the law enforcement community is the future widespread use of cryptographic technology in criminal activity and the enormous impediment that creates in the electronic surveillance arena.[164] Also, the Court would scrutinize the administrative procedures to determine if there was proper protection of the encryption keys. Given the recent public disclosure regarding the set-up of the key escrow system, it would seem that the government has developed adequate procedural safeguards to ensure the protection of keys from improper disclosure.[165] The Court might note the fact that two key components are split between two escrow agents and are not personally identifiable to the key escrow agents. The key components are received by an authorized law enforcement official in encrypted form sent directly to a "blackbox" in order to maintain confidentiality of the key components that make up the decryption key.

The government is not collecting evidently personal information. The escrowed key components are not related to particular individuals. The chip keys are not formed and related to individuals until they are used, and they are discarded after use. Because the government is not developing a database

---

159. See discussion of *Whalen*, *Nixon*, and *Reporter's Committee* cases.

160. Franks, *The National Security Agency and Its Interference with Private Sector Computer Security*, 72 Iowa L. Rev. 1015, 1017 (1987).

161. Id.

162. Id.

163. *Terry v. Ohio*, 392 U.S. 1, 9 (1968); *Katz*, 389 U.S. 347, 360-61.

164. Meeting of the Computer System Security and Advisory Board, July 29-30, 1993, at the National Institute of Standards and Technology, Briefing by Law Enforcement Community on Cryptography.

165. Meeting of the Computer System Security and Advisory Board, July 29-30, 1993, at the National Institute of Standards and Technology, Briefing by Geoffrey Greiveldinger, Special Counsel, Narcotic and Dangerous Drug Section, Department of Justice.

of personal information, the requirement of privacy may not apply.

However, the proposed government key escrow system could be construed as the collection, use, and maintenance of personal information, whereby the prescribed key escrow agents (i.e., presumably a federal agency) could be subject to the requirements of the Privacy Act. Even though the government would only directly control the encryption keys and not the information itself, the maintenance and use of the keys are intimately related to the access of private encrypted information. The Privacy Act's main goal was to protect an individual interest in controlling the use of personal information after its release to the government.[166] One of these requirements prohibits any federal agency from disclosing any information contained in a system of records, without written consent of the individual to whom the record pertains. Yet, the scope of this prohibition on nonconsensual disclosure is subject to numerous exemptions. Specific exemptions exist for law enforcement purposes in response to exigent circumstances, although keys may only be released through Title III and the Federal Information Security Agency. However, the routine use exemption as used by the CIA must be scrutinized closely by the Court for its potentially perilous impact on the key escrow system.[167]

1.2 SECOND AMENDMENT?RIGHT TO BEAR ARMS

1.2.1 General Issues

1.Should cryptographic technology be categorized as a weapon, such as a gun, and thus regulated by the right to bear arms under the second amendment?

1.2.2 State of the Law

The Second Amendment states that “a well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.”[168] It is an area of “constitutional jurisprudence that still awaits its philosopher.”[169] The Supreme Court has directly ruled on the Second Amendment in only four cases.[170] The first three cases have recognized the individual right and a bar to federal infringement of the right. The Court in *Miller* limited the Amendment protection to weapons useful for militia duty. Since then, lower federal courts have heard Second Amendment claims, often dismissing them on grounds that the Amendment has not been incorporated into the Fourteenth Amendment, which would make it binding on the states. Most of these cases pertained to persons involved in criminal activity who were also convicted of firearms charges; thus these cases were not really a “good test of the extent to which the Second Amendment protects the rights of the public at large.”[171]

166.Note, *supra*, at 143.

167.5 U.S.C. § 552a(b)(8).

168. U.S. CONST. amend. II.

169.Cottrol, Robert J., Raymond J. Diamond, *The Second Amendment: Toward an Afro-Americanist Reconsideration*, 80 Geo. L. J. 309, 310 (1991).

170.*Miller v. Texas*, 153 U.S. 5353 (1984); *U.S. v. Miller*, 307 U.S. 174 (1939); *Presser v. Illinois*, 116 U.S. 252 (1886); *U.S. Cruishank*, 92 U.S. 542 (1876).

171.Cottrol, *supra*, at 312 n.3.

One legal scholar has recently examined the Second Amendment within the context of the Bill of Rights and concluded the purpose of the Amendment as preventing Congress from disarming freedmen, so that the public could resist tyranny by a standing army.[172] However, some scholars believe the purpose of the Second Amendment was to maintain the militia, not to provide an individual right to bear arms.[173] Opponents of stricter gun controls tended to stress the Amendment's clause arguing that the framers intended a militia of the whole, who was expected to perform its duties with privately owned weapons.[174]

1.2.3 General Issues Addressed

Currently, courts have not addressed the regulation of cryptography in the context of a right to bear arms under the Second Amendment. However, cryptographic technology is listed as a munition on the U.S. Munitions List promulgated by the AECA. Nevertheless, cryptography would have to fall into the limitation imposed by *Miller*, thereby construing cryptography as a weapon useful for militia duty.[175]

1.3 FOURTH AMENDMENT

1.3.1 Search and Seizure of Stored Communications and Data

1.3.1.1 General issues

1.May the government seize encrypted electronic/computer stored documents or papers without prior notification to owner?

2.Does requiring disclosure of the encryption key to the government in advance of there being probable cause sufficient to allow the government to seize an encrypted stored communication and to search and seize the key to such communication violate the Fourth Amendment?

1.3.1.2 State of the law

The Fourth Amendment states that the "right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . ."[176] This right protects individuals against arbitrary invasions of their privacy by law enforcement officials, thus preserving a balance between the needs of law enforcement and those of individuals.[177] The Amendment restricts searches and seizures that infringe upon an individual's reasonable expectation of privacy;[178] with a few exceptions, a search warrant must be obtained prior to a search.[179] Law enforcement officials are not required to obtain warrants for every search. The police do not need

172. *Id.* at 312 n.5.

173. *Id.* at 313.

174. Id.

175. 307 U.S. at 180.

176. U.S. CONST. amend. IV.

177. Retz C., *Warrant Requirement for Searches of Computerized Information*, 67 B.U. L. Rev. 179, 180 (1987).

178. *Terry v. Ohio*, 392 U.S. 1, 9 (168).

warrants to conduct certain searches of automobiles, searches incident to a lawful arrest, searches in emergency, or situations involving hot pursuit.[180]

The courts used to construe the Fourth Amendment to protect only tangible property against physical searches and seizures.[181] In 1967, the Supreme Court in *Katz v. United States*[182] explicitly rejected the *Olmstead* view, stating the Fourth Amendment protects "people" not simply "places" against unreasonable search and seizure. "What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection."[183] The Supreme Court has subsequently held that a "search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[184] Whether a person has standing to contest a search on Fourth Amendment grounds depends on whether the person had a legitimate expectation of privacy in the area searched, not merely in the items seized.[185]

The Electronic Communications Privacy Act (ECPA) amended Title III of the Omnibus Crime Control and Safe Street Act. The ECPA extends the reach of Title III to electronically stored information. The Act makes unlawful access to stored communications, when a person intentionally accesses without authorization a "facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" and thus obtains, alters, or prevents authorized access to a wire or electronic communication while it is in storage in such system."[186] Exceptions to this prohibition are made for entities providing "wire or electronic communications service," an "intended" user, or an authorized government law enforcement officer.[187]

Section 2703 outlines the requirements for governmental access. The government may require the disclosure by a provider of electronic communication service of the contents of a communication in electronic storage, pursuant to a warrant.[188] The government may require a "provider" of remote computing services to disclose contents of an electronic communications, pursuant to a warrant, without prior notice to the "subscriber" or "customer."[189]

1.3.1.3 General issues addressed

---

179. *Stanley v. Georgia*, 394 U.S. 557 (1969). The Fourth Amendment explicitly provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

180. Retz, *supra*, at 184-85.

181. *Olmstead v. United States*, 277 U.S. 438 (1928).

182. 389 U.S. 347, 352 (1967).

183. *Id.*

184. *United States v. Karo*, 486 U.S. 705, 712 (1984); *Katz*, 389 U.S. at 361. (First time the Court outlined a twofold test to determine what protections are afforded to people under the Fourth Amendment. The first prong required that the individual exhibit an actual expectation of privacy, and the second prong required that the expectation be one that society is prepared to recognize.)

185. *United States v. Skowronski*, 827 F.2d. 1414 (1987).

186. 18 U.S.C. §§ 2701(1), (2).

187. *Id.* at §§ 2701(c)(1), (2), 2702(b)(6).

188. *Id.* at § 2703(a).

189. *Id.* at § 2703(b).

First general issue. The first general issue?May the government seize encrypted electronic/ computer stored documents or papers without prior notification to owner??is addressed by the ECPA on two levels, depending on the forum in which the electronic communication is being stored. Section 2703(a) specifically states that an authorized government agency "may require the disclosure by a provider of electronic communication of the contents of electronic communication" in electronic storage, pursuant to a warrant.[190] The contents of electronic communications that are "held or maintained on that service" in a remote computing service environment can be disclosed to an authorized government entity without required notice to the "subscriber" or "customer" of this type of service, with a proper warrant.[191] The ability to seize does not depend on the form of the contents of electronic communication at time of seizure; thus encrypted speech is governed by this statute.

Second general issue. When the second general issue?Does requiring disclosure of the encryption key to the government in advance of there being probable cause sufficient to allow the government to seize an encrypted communication and to search and seize the key to such communication violate the fourth amendment??is considered, given the current available information on the procedures governing key escrow technology, a question arises: Is the government requiring disclosure of an encrypted key prior to sufficient probable cause? For each cryptographic device, the government has two key escrow agents. Each agent will possess a unique encrypted component of the chip key along with the identification number particular to that chip. Thus, an individual agent does not have the capability to combine the components necessary to form a chip key. Once proper authorization has been secured by law enforcement and key escrow encryption technology has been identified, this chip key can be secured by law enforcement to be used to decrypt the contents of a communication. Therefore, a question arises regarding whether individuals are surrendering their encryption keys prior to the determination of probable cause. The system currently being proposed is analogous to a system of registration by the government so that it can maintain an ability to access the contents of stored electronic communications.[192]

1.3.2 Search and Seizure of Voice and Data Transmission

1.3.2.1 General issues

1.In a situation were one or both users of the proposed key escrow system are located outside U.S. borders, does a warrant requirement exist for the U.S. Government to seize voice or data communication between the users?

2.Does requiring disclosure of the encryption key to the government in advance of there being probable cause sufficient to allow the government to seize an encrypted transmitted communication and to search and seize the key to such communication violate the Fourth Amendment?

1.3.2.2 State of the law

In *Berger v. New York*, the Supreme Court discussed the guidelines for authorization of interception of communications. To obtain authorization, the law enforcement official must particularly describe

190.*Id.* at § 2703(a).

191.*Id.* at §§ 2703(b)(1)(A), (B), (b)(2), (b)(2)(A).

192.*Id.*

the place to be searched and the persons or things to be seized, and the official must show probable cause sufficient to warrant a person of reasonable caution to believe that an offense has been or is being committed.[193] The order must describe "the type of conversation sought with particularity," by indicating the specific objective of the government in "entering the constitutionally protected area" and the limitations placed upon the officer executing the warrant.[194] The limitations placed on the officer provide that the officer does not search unauthorized areas and that the officer only seizes the property sought.[195] The order must also limit the intrusion, and a new order may be issued if probable cause is shown for a succeeding period of intrusion.[196] The officer must make a report of how the order was executed and what was seized.[197] The Court believed through these precautions that the "danger of an unlawful search and seizure was minimized," thus allowing the search to be within the limits of the Fourth Amendment.[198]

Title III of the Omnibus Crime Control and Safe Street Act. In formulating Title III of the Omnibus Crime Control and Safe Street Act [hereinafter referred to as "Title III"],[199] Congress attempted to balance two important interests: the legitimate needs of the law enforcement and the privacy concerns of the public.[200] Thus, Congress outlined a comprehensive scheme for regulating the interception of wire or oral communications.

Title III prohibits the use of any "electronic, mechanical, or other device" for the interception of communications,[201] and such devices can be seized or confiscated by the United States.[202] This prohibition applies to all private eavesdropping and governmental eavesdropping without a court order. It prescribes a punishment of a maximum fine of $10,000, imprisonment for 5 years, or both for any person who willfully intercepts a wire or oral communication, discloses the contents of an intercepted communication, or uses such contents.[203] Furthermore, any attempt to commit, or solicit another to commit, any of the above acts is a separate offense.[204]

Section 2511(2) provides certain exceptions to the broad prohibitions of § 2511(1), permitting interception where the speaker has given prior consent, or by employees of the Federal Communications Commission (FCC), a common carrier in the ordinary course of monitoring duties, or a "person acting under the color of the law to intercept a wire or oral communication."[205]

---

193. 388 U.S. 41, 57.

194. Id.

195. Id.

196. Id.

197. Id.

198. Id.

199. 18 U.S.C. § 2510 et seq.

200. Balmforth, Kathyrn and Michael Goldsmith, *The Electronic Surveillance of Privileged Communications: A Conflict in Doctrine*, 64 S. Cal. L. Rev. 903, 904; see Carr, J.G., *The Law of Electronic Surveillance 1-8 to 2-13* (1989), for a discussion of the history of electronic surveillance in the judicial system and development of Title III.

201. *Id.* at § 2511(1)(b).

202. *Id.* at § 2513.

203. 18 U.S.C. § 2511(1).

204. Id.

xxx

To perform eavesdropping, the principal federal or state prosecutor must apply to a judge of competent jurisdiction for an eavesdrop order.[206] The judge must find probable cause as to the commission of a crime, the likelihood of intercepting relevant communications, and the failure of ordinary investigation.[207] All orders must be limited in time.[208] However, a temporary delay in obtaining the eavesdrop order may be allowed in an exigent situation threatening the national security interest or characteristic of organized crime, as long as application is made within 48 hours.[209]

Title III imposes an exclusionary rule on all eavesdrop evidence seized without a court order. The rule requires that "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States . . . if the disclosure of that information would be in violation of this chapter."[210]

The following are pertinent definitions as used in Title III.

•**Wire communication**?any communication made in whole or part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and point of recognition furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.[211]

•**Oral communication**?"any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[212]

•**Intercept**?the "aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."[213]

•**Contents**?with respect to wire or oral communication, consists of "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication."[214]

•**Investigative or law enforcement officer**?any officer of the United States or of a state or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for

205. *Id.* at §2511(2)(d).
206. *Id.* at § 2516.
207. *Id.* at § 2518(3).
208. *Id.* at § 2518(5).
209. *Id.* at § 2518(7).
210. *Id.* at § 2515.
211. *Id.* at § 2510(1).
212. *Id.* at § 2510(2).
213. *Id.* at § 2510(4).
214. *Id.* at § 2510(8).

offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.[215]

The legislative history of Title III stated that "the major purpose of Title III is to combat organized crime" and cited the hardship in obtaining proof as the primary reason for the lack of success in prosecution of this type of criminal activity.[216] Six years after the passage of Title II, the National Wiretap Commission evaluated the effectiveness of the statute.[217] The majority of the Commission strongly reaffirmed the finding of Congress during the enactment of Title III in 1968 that electronic surveillance is an "indispensable aid" to law enforcement in finding evidence of crimes perpetuated by organized criminals.[218] In 1986 the President's Commission on Organized Crime reinforced the opinion that electronic surveillance is critical to the successful investigation and prosecution of organized crime.[219]

Foreign Intelligence Surveillance Act. In *Katz*, the Court expressly preserved national security surveillance from the reach of its decision that a warrant would be required for electronic surveillance.[220] Justice White noted the unique requirements of electronic surveillance for national security purposes, concluding no prior judicial review should be required if the President or the Attorney General found surveillance reasonable under the circumstance.[221]

This distinction between law enforcement and national security requirements for electronic surveillance was subsequently recognized by Congress as well. In enacting Title III, Congress specifically disclaimed any intention that its provisions, or those of the Communications Act of 1934, should be construed to affect the constitutional powers of the President to protect the United States against hostile powers, to obtain foreign intelligence information, or to protect against any other "clear and present danger."[222]

In the leading case on this issue, *United States v. United States District Court*, the Court concluded that the reservation of Presidential authority in Title III represented merely a neutral statement by Congress that the President has some degree of power in the national security area and was not an attempt to expand, define or contract that power.[223] Thus, it was necessary to review the constitutional authority, rather than a statutory basis for surveillance authority.[224] The Court never addressed the legality of the Executive to undertake warrantless electronic surveillance for national security purposes.

---

215. *Id.* at § 2510(7).

216. See Title III Senate Report No. 1097, 90th Cong., 2d Sess., reprinted in 1968 U.S. Code Cong. & Admin. News 2112, 2154-57.

217. National Wiretap Commission, Electronic Surveillance: Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance 33-40 (1976).

218. *Id.* at xiii; see Balmforth, *supra*, at 907.

219. Balmforth, *supra*, at 907.

220. 389 U.S. at 358 n.23.

221. *Id.* at 363-64.

222. 18 U.S.C. § 2511(3).

223. 407 U.S. 297, 303-08 (1972).

224. *Id.* at 406.

Subsequently, Congress enacted the Foreign Intelligence Surveillance Act, which provides exclusive means of authorizing various types of electronic surveillance for national security purposes. Activities must be authorized in advance by one of the seven district court judges designated by the Chief Justice of the Supreme Court as members of the Foreign Intelligence Surveillance Court (FISC).[225] The government presents warrants in camera, ex parte proceedings conducted under physical security measures designed to protect sensitive national security information.[226] The Chief Justice also designates three federal appeals court judges to review government appeals in instances in which FISC judges have denied applications for warrants.[227]

All applications to FISC require the Attorney General's approval.[228] The FISC judge must find the location at which the surveillance is directed and the procedures proposed by the government adequately minimize the acquisition, retention, and dissemination of information concerning unconsenting persons.[229] The application must be accompanied by an official statement for senior government officials that the information sought relates to national defense or foreign relations.[230]

The Act also contains detailed provisions specifying the requirements and procedures mandated when information is intended to be used in a criminal proceeding. Barring such situations or an emergency surveillance approval by the Attorney General, there is no requirement to give notice to any target concerning the fact the government has conducted such surveillance.[231]

1.3.2.3 General issues addressed

First general issue. Regarding the first general issue?In a situation when one or both users of the proposed key escrow system are located outside U.S. borders, does a warrant requirement exist for the U.S. government to seize voice or data communication between the users??the Supreme Court has held that the Fourth Amendment, particularly its warrant requirement, is inapplicable outside the United States.[232] Given the proposed key escrow system, obtaining a warrant under Title III for electronic surveillance if one of the sources is located in the United States should present no problem. The government in this instance would wiretap only the line of the source located in the United States. Thus, only in the case where both sources are located outside the United States is it not clear that a warrant requirement exists.

Second general issue. Regarding the second general issue?Does requiring disclosure of the encryption key to the government in advance of there being probable cause sufficient to allow the government to seize an encrypted transmitted communication and to search and seize the key to such communication violate the fourth amendment??see the discussion above in a stored communications context.[233] The system currently being proposed is analogous to a system of registration by the government so that it can maintain its ability to perform electronic surveillance.[234]

---

225. 50 U.S.C. § 1801 et seq.

226. *Id.* at §§ 1804(a), 1805(a), 1803(c).

227. *Id.* at § 1803(b).

228. *Id.* at §§ 1804(a), 1805(a)(3).

229. *Id.* at §§ 1804(a)(4)(B), (5), 1801(h).

230. *Id.* at §§ 1804(a)(7), 1801 (e)(2).

231. *Id.* at § 1806(j).

232. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990).

1.4 FIFTH AMENDMENT?SELF INCRIMINATION

1.4.1 General Issue

1.Does a key escrow system that may involuntarily secure from the user the key to decipher the user's encrypted messages violate the Fifth Amendment's privilege against self-incrimination?

1.4.2 State of the Law

The Fifth Amendment, in relevant part, states that "[n]o person . . . shall be compelled[235] in any criminal case to be a witness against himself."[236] In *Fisher v. United States*, 425 U.S. 391 (1976), the Court framed the modern interpretation of Fifth Amendment privilege. The Court held that the compelled production of documents, even if the contents are incriminating, does not violate the Fifth Amendment unless the person is compelled to make a testimonial communication.[237]

The production of incriminating evidence. The Court in *Fisher* noted that the compelled production of evidence containing incriminating evidence did not automatically invoke Fifth Amendment privilege. The Court stated that the "Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating."[238] The Court recognized that "[a] subpoena served on a taxpayer requiring him to produce an accountant's workpapers in his possession without a doubt involves substantial compulsion. But it does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought."[239] The Court further stated that the Fifth Amendment would not be violated "by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications."[240]

The Court analyzed the voluntary nature of the evidence produced. With respect to the papers being subpoenaed, "the preparation of all of the papers sought . . . was wholly voluntary, and they cannot

---

233. See *supra*, p. 35.

234. 50 U.S.C. § 2511(2).

235. "Word `compel' as used in constitutional right to be free from being compelled in a criminal case to be a witness against one's self means to be subjected to some coercion, fear, terror, inducement, trickery or threat?either physically or psychologically, blatantly or subtly; the hallmark of compulsion is the presence of some operative force." Black's Law Dictionary.

236. U.S. CONST. amend. V.

237. "In order to be `testimonial,' an accused's oral or written communication, or act, must itself, explicitly or implicitly, relate a factual assertion or disclose information. It is consistent with the history of and the policies underlying the Self-Incrimination Clause to hold that the privilege may be asserted only to resist compelled explicit or implicit disclosures of incriminating information." *Doe v. United States*, 487 U.S. 201 (1988).

238. *Fisher v. United States*, 425 U.S. 391, 408 (1976).

239. *Id.* at 409.

240. *Id.* at 409.

be said to contain compelled testimonial evidence, either of the taxpayers or of anyone else."[241] "The fact that the documents may have been written by the person asserting the privilege is insufficient to trigger the privilege, . . . [a]nd unless the Government has compelled the subpoenaed person to write the document, the fact that it was written by him is not controlling with respect to the Fifth Amendment issue."[242] In essence, the government cannot compel a person to involuntarily create evidence to incriminate himself, whether in the form of a written admission of guilt, development of document, etc. But the government may compel the production of voluntarily created documents, even if documents are self-incriminating.[243]

Fifth Amendment and the Fourth Amendment's Right to Privacy and Protection from Unreasonable Search and Seizure. The Court commented on the relationship between the Fifth Amendment's self-incrimination clause and the Fourth Amendment's privacy and unreasonable search and seizure clauses. The Court, in its analysis of privacy, recognized that "one of the several purposes served by the constitutional privilege against compelled testimonial self-incrimination is that of protecting personal privacy. . . . But the Court has never suggested that every invasion of privacy violates the privilege. Within the limits imposed by the language of the Fifth Amendment, . . . the privilege truly serves privacy interests; but the Court has never on any ground, personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which . . . did not involve compelled testimonial self-incrimination of some sort[244] . . . . We cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy?a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. We adhere to the view that the Fifth Amendment protects against `compelled self-incrimination, not [the disclosure of] private information.'"[245]

With respect to self-incrimination and unreasonable search and seizure, the Court commented on a line of cases in which the Fifth Amendment was offended by the use of evidence of documents or property seized in violation of the Fourth Amendment.[246] However, the Court in those cases also found elements of compelled self-incrimination.[247] "[I]n either case he is the unwilling source of the evidence, and the Fifth Amendment forbids that he shall be compelled to be a witness against himself in a criminal case."[248]

The Court also noted that "under the appropriate safeguards private incriminating statements of an accused may be overheard and used in evidence, if they are not compelled at the time they were uttered.[249] . . . [W]hen the state['s] reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue."[250]

---

241. *Id.* at 409-410.

242. *Id.* at 410 n. 11.

243. See *United States v. Doe*, 465 U.S. 605, 612 n.10 ("If the party asserting the Fifth Amendment privilege has voluntarily compiled the document, no compulsion is present and the contents of the document are not privileged").

244. *Id.* at 399.

245. *Id.* at 401 [quoting *U.S. v. Nobles*, 422 U.S. 225, 233 n.7 (1975)].

246. *Id.* at 399, n.5. See *Gouled v. United States*, 55 U.S. 298 (1921); *Agnello v. United States*, 269 U.S. 20 (1925); *United States v. Lefkowitz*, 285 U.S. 452 (1932).

247. Id.

248. *Gouled*, 255 U.S. at 306.

1.4.3 Conclusion

1.Does the compelled production of a “key” to decipher encrypted messages amount to self-incrimination as defined by the Fifth Amendment?

Although there are no cases that directly address this issue, it appears from past decisions that the government's compelled production of a “key” to decipher messages would not violate the Fifth Amendment's privilege against forced self-incrimination. The procurement of the key itself is not testimonial in nature, and it in no way incriminates the person from whom the key is procured. But, even if it can be concluded that the procurement of the key is in essence the procurement of the communication to be deciphered, the Court has stated that if the communication was voluntary, no right has been abridged by the government's compelled production of that evidence. In *Doe v. United States*, the Court noted that if a compelled statement is “not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence.”[251] Also in *Doe v. United States*, Justice Stevens, in his dissenting opinion, observed that a person “may in some cases be forced to surrender a key to a strongbox containing incriminating documents.”[252] This analogy fits well with the key escrow function and lends further support to its constitutionality on Fifth Amendment grounds.

2. U.S. CONTROLS ON ENCRYPTION TECHNOLOGY

2.1 DOMESTIC CONTROLS

2.1.1 Computer Security Act of 1987

The Computer Security Act requires federal agencies to identify and develop security plans for computer systems that hold sensitive information. The Act intended to prevent persons from illegally tapping into government computer systems and altering or destroying records.[253] The Act gives the National Institute of Standards and Technology (NIST) responsibility for promulgating guidelines to protect the security of sensitive but unclassified computer information.[254] The term “sensitive information” means any nonsecret information that could adversely affect the national interest, the conduct of federal programs, or rights created under the Privacy Act. [255]

249.See *Katz v. United States*, 389 U.S. 347 (1967); *Osborn v. United States*, 385 U.S. 323 (1966); *Berger v. New York*, 388 U.S. 41 (1967).

250.*Fisher*, 425 U.S. at 400.

251.*Doe v. United States*, 487 U.S. 201, 208 n.6 (1988) (quoting *In re Grand Jury Subpoena*, 826 F.2d 1172, n.2 (concurring opinion).

252.*Id.* at 219 (Justice Stevens dissenting opinion).

253.Note, *Nineteenth Annual Administrative Law Issue: Developments under the Freedom of Information Act*, 1988 Duke L.J. 566 (1987).

254.Id.

255.H.R. 145, 100th Cong., 1st Sess. § 3(c)(4), 133 Cong. Rec H5340 (daily ed. June 22, 1987).

2.1.2 Brooks Act

The Brooks Act was enacted to ensure the "economic and efficient" procurement of automated data processing and telecommunications equipment (ADPTE) by federal agencies. All computer supplies and services as well as telecommunications equipment fall into the ADPTE category.[256] The General Services Administration is responsible for providing ADPTE to federal agencies either directly or under a delegation of procurement authority.

Over the Act's 25-year history, the most important development involved the ability for certain agencies to exempt themselves from ADPTE purchasing requirements. The Warner Amendment passed in 1981 exempted certain Defense Department purchases from the Brooks Act provisions.[257] These purchases included any Defense Department procurements "critical to the direct fulfillment of military or intelligence missions" of the United States or in which the ADPTE exists as an "integral part of a weapon or weapons system;" these purchases also included "cryptologic activities related to national security."[258]

NIST provides cryptographic technology for unclassified government information primarily pursuant to the Brooks Act.[259] The Act explicitly grants control over national security information data processing needs to the President, who in turn has delegated that task to the NSA or other military agencies.[260]

2.2 EXPORT CONTROLS

2.2.1 Arms Export Control Act, 22 U.S.C. § 2778

The AECA is the statutory authority that governs export controls of defense articles and services to foreign countries. The purpose of the AECA is to control the export of defense articles that may contribute to an arms race, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control arrangements.[261] Thus, "[i]n 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. . . . The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services."[262]

---

256. Marshall, Robert C., Michael J. Meurer, Jean-Francois Richard, *The Privacy Attorney General Meets Public Contract Law: Procurement Oversight by Protest*, 20 Hofstra L. Rev. 1, 34 (1991).

257. Department of Defense Authorization Act of 1982 (Warner Amendment), Pub. L. No. 97-86, § 908(a)(1), 95 Stat. 1099, 1117 (1981) (amended 1982), codified as 10 U.S.C. § 2314 (1988).

258. *Id.* at § 2315(a); see Marshall, *supra*, at 35.

259. Franks, Renae A., Note, *The National Security Agency and Its Interference with the Private Sector Computer Security*, 72 Iowa L. Rev. 1015, 1019 (1987).

260. *Id.*; see *U.S. v. Curtiss-Wright*, 299 U.S. 304, 319 (1936) (the President's power over national security is based on his constitutional authority in foreign relations).

261. 22 U.S.C. § 2778 (a)(2).

262. 22 U.S.C. § 2778 (a)(1).

2.2.1.1 International Traffic in Arms Regulations

The ITAR, 22 C.F.R. §§ 120-130, promulgates the policies set forth in the AECA. The State Department is given exclusive regulatory authority to carry out the ITAR by the President.

U.S. Munitions List. Items considered defense articles and services appear in the U.S. Munitions List,[263] and individual validated export licenses must be approved for these items. The designation of items to appear on the Munitions List is handled by the State Department in concurrence with the Defense Department. Designations of articles to the Munitions List is based primarily on whether the article or service is deemed to be inherently military in character. Whether an item is used for both military and civilian purposes does not determine whether it will be placed on the list. Also, the intended use of the article is not relevant in determining whether an item will be subject to restrictions.[264]

The determination of items to be placed on the Munitions List is not judicially reviewable.[265] However, the AECA provides for periodic review of items appearing on the Munitions List to determine which items no longer warrant export restrictions under the AECA and ITAR. For an item on the Munitions List to be decontrolled, a request to remove the item from the list must be received by the State Department. The State Department reviews the item with the appropriate agencies and determines whether the item should be decontrolled. Items decontrolled by the State Department may be placed on the Commerce Control List, and control of these items accordingly shifts to the Commerce Department.[266]

Export licenses. Defense items appearing on the Munitions List are under the exclusive jurisdiction of the State Department. Those wishing to export items on the Munitions List must be registered with the State Department prior to submitting an export license application. Any person intending to export a defense article must obtain an individually validated license from the State Department prior to each export. An application for the permanent export of defense articles sold commercially must be accompanied by a purchaser order, letter of intent, or any other appropriate documentation.[267] With respect to distribution warehouses, the initial agreement for warehousing and distributing defense articles must be approved by the State Department before they enter into force. The agreement must contain conditions for special distribution, end-use, and reporting and must specify the terms and conditions in which the article will be exported, the duration of the agreement, and the countries involved in the distribution territory.[268] Licenses for exports pursuant to a distribution agreement must be approved prior to export.

An export license is required for the export of unclassified technical data. A license must be obtained for any oral, visual, or documentary disclosure of technical data to foreign nationals during visits to foreign countries by U.S. persons, visits by a foreign national to the United States, or any other situation. A license is required regardless of the manner in which the technical data are transmitted, whether the transfer be in person, by telephone, through correspondence, or electronically.[269]

---

263. 22 C.F.R. § 121.1.

264. 22 C.F.R. § 120.3.

265. 22 U.S.C. § 2778 (h).

266. 22 U.S.C. § 2778(f).

267. 22 C.F.R. § 123.1.

268. 22 C.F.R. § 124.14 (a)-(b).

However, information which is in the public domain[270] is not subject to the controls for technical data.

In determining whether to issue an export license, consideration must be given to whether an article will contribute to the arms race, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral arms control arrangements. When considering applications, recommendations from other agencies may be sought. These recommendations are used to aid in determining whether to grant export licenses.

Violations and penalties. The export or attempt to export any defense article or technical data or to furnish any defense service for which a license is required without obtaining the required license or violating any of the terms or conditions of a granted license is prohibited under the ITAR.[271] Persons granted export licenses are responsible for the acts of their employees, agents, and all persons entrusted with the operation, use, possession, transportation, and handling of licensed defense articles or technical data abroad.[272]

It is also a violation for a person to knowingly apply for a license, or order, buy, receive, use, sell, deliver, store, dispose of, forward transport, finance, or otherwise participate in any transaction involving a defense article or technical data, for the benefit directly or indirectly of a person facing debarment or suspension.[273] In addition, it is unlawful for a person to willfully aid, abet, cause, counsel, demand, induce, procure, or permit the commission of any act prohibited by the ITAR.[274] It is also unlawful to use any export control document containing false statements, misrepresentations, or omissions of material facts for the exporting of any defense article or technical data or the furnishing of any defense service for which a license is needed.[275]

Any person willfully violating any part of the AECA or the ITAR or, in a registration, license application, or report, willfully making untrue statements of a material fact, omitting a material fact, or making misleading statements shall, upon conviction, be subject to fine, imprisonment, or both.[276] For criminal offenses, the fine shall be not more than $1,000,000 or imprisonment not more than 10 years, or both, for each violation.[277] Civil penalties shall be in accordance with those set forth in the Export Administration Act, 50 U.S.C.S. App. 2410 (c), which may not exceed $500,000 for each violation.[278] Civil penalties may be in addition to or in lieu of any other liability or penalty which may be imposed.

U.S. Customs may take the appropriate steps to enforce the regulations set forth in the ITAR. U.S. Customs may inspect the loading or unloading of any vessel, aircraft, or vehicle or order the

---

269. 22 C.F.R. § 125.2 (c).
270. 22 C.F.R. § 120.18.
271. 22 C.F.R. § 127.1 (a)(1), (3).
272. 22 C.F.R. § 127.1 (b).
273. 22 C.F.R. § 127.1 (c)(1)-(2).
274. 22 C.F.R. § 127.1 (d).
275. 22 C.F.R. § 127.2 (a).
276. 22 C.F.R. § 127.3.
277. 22 U.S.C. § 2778(c).
278. 22 C.F.R. § 127.9(a).

production of any relevant documents or information pertaining to a particular export.[279]

2.2.1.2 ITAR controls on encryption technology

Category XIII(b)(1) of the Munitions List covers cryptographic equipment. Originally section (b)(1) of the category consisted of "[s]peech scramblers, privacy devices, cryptographic devices and software (encoding and decoding), and components specifically designed or modified therefore, ancillary equipment, and protective apparatus specifically designed or modified for such devices, components, and equipment." Recent amendments to the ITAR have decontrolled specific categories of cryptographic equipment. These amendments removed cryptographic technology involving message authentication, access control devices, television descramblers, automatic teller machines, virus protection, and "smart cards," and placed these items under Commerce Department jurisdiction. Also, certain (but not all) types of mass-market software have been decontrolled. All other items remain under State Department jurisdiction.[280]

Export applications involving cryptography are reviewed by the State Department and then reviewed by the Defense Technology Security Agency, the Energy Department, the appropriate Military Services, and the NSA. The application must include the proposed use of the item and the end user of the item. Recommendations from the aforementioned agencies to approve or reject the application are then sent to the State Department, and the State Department makes the final decision on the license.

Certain types of mass market software still under State Department control may be approved on an expedited basis. Software involving RC2/RC4 algorithms may be approved in 7 days, whereas other software may be approved in 15 days. Also, other less powerful algorithms may appear on an "automatic" list, which is a list of commonly approved noncritical items still under the control of the State Department which are immediately approved. The Data Encryption Standard (DES) and other strong algorithms are not eligible for approval under this schedule. DES may be approved for financial institutions and U.S. subsidiaries through the normal approval process. However, generally cryptographic technology used to encrypt data is not approved. Only those used for message authentication and access control are approved.

2.2.2 The Export Administration Act of 1979, 50 U.S.C.S. app. §§ 2401-2420

The EEA of 1979 and its subsequent amendments are designed to strengthen the international commercial commerce position of the United States. This Act implements policies designed to "minimize uncertainties in export control policy and to encourage trade with all countries with which the United States has diplomatic or trading relations, except those countries with which such trade has been determined by the president to be against the national interest."[281] This policy was based on the findings of Congress that "[e]xports contribute significantly to the economic well-being of the United States and the stability of the world economy by increasing employment and production in the United States, and by earning foreign exchange, thereby contributing favorably to the trade balance. . . . It is important for the national interest of the United States that both private sector and

---

279. 22 C.F.R. § 127.4.

280. See Interim Final Rule, amendments to ITAR, 57 Fed. Reg. 32148, July 20, 1992; Final Rule, amendments to ITAR, 57 Fed. Reg. 15227, April 27, 1992.

281. 50 U.S.C. app. § 2402.

the Federal Government place a high priority on exports, consistent with the economic, security, and foreign policy objectives of the United States."[282]

As a result of these and other findings and policy considerations, the EEA declares that restrictions on exports may be used
only after full consideration of the impact on the economy of the United States and only to the extent necessary?
(A) to restrict the export of goods and technology which would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States;
(B) to restrict the export of goods and technology where necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations; and
(C) to restrict the export of goods where necessary to protect the domestic economy from the excessive drain of scarce materials and to reduce the serious inflationary impact of foreign demand.[283]

2.2.2.1 Export Administration Regulations

The EARs, 15 C.F.R. parts 768-799, promulgate the policies set forth by the EEA. The Commerce Department is given regulatory authority over the export control of commodities.

Commerce Control List. Commodities under the control of the Commerce Department appear on the Commerce Control List (CCL). The Commerce Department requires export licenses for the export of goods or technologies that appear on the CCL. Licenses that may be required include (1) a validated license for a specific export; (2) a validated license for multiple exports, which include distribution licenses, comprehensive operations licenses, project licenses, and service supply licenses (see 50 U.S.C.S. app. 2403); (3) a general license; and (4) other licenses as required under the EEA.

The following groups of items are not controlled under the EARs and do not appear on the CCL:

•U.S. Munitions List,
•narcotics and dangerous drugs,
•commodities subject to Atomic Energy Act,
•watercraft,
•natural gas and electric energy,
•tobacco seeds and plants,
•endangered fish and wildlife, and
•patent applications (secrecy orders).

Export Licenses. The export of all commodities appearing on the CCL and technical data[284] requires a general license (if established) or a validated license or other authorization for export granted by the Office of Export Licensing, except for the following:

•any export to Canada for consumption in Canada, unless an individual validated license is required;

---

[282]. 50 U.S.C. app. § 2401.
[283]. 50 U.S.C. app. § 2402.
[284]. As defined in 15 C.F.R. § 779.1.

•exports for the official use of or consumption by the U.S. Armed Forces; and

•exports of commodities and technical data controlled by another U.S. agency.[285]

A general license is one for which no application is required and for which no document is granted or issued. It is available for use by all persons, except by those specifically prohibited from exporting commodities.[286] These general licenses are only applicable to exports under the licensing authority of the Commerce Department.[287]

A validated license is a document issued by, or under the authority of, the Commerce Department authorizing a specific export.[288] Types of validated licenses include (1) individual license, (2) project license, (3) distribution license, (4) service supply license, and (5) special chemical license.[289]

The Commerce Department will, when applicable, consult with other appropriate agencies before approving an export application requesting a validated license. Foreign policy concerns (which involve restrictions of certain exports to certain countries) and national security concerns will be taken into consideration when an application is being evaluated.[290] If an application is denied, notification will be provided within 5 days to the applicant. The notice will state the statutory basis for the denial, the policies that will be furthered by the denial, the specific considerations which led to the denial, and the availability of appeal procedures.[291] The EARs provide procedures for appeals of denied applications.

The Commerce Department reviews items on the CCL at least every 3 years for multilateral controls and every year for all other controlled commodities. In the review, commodities presently under the validated license control are reviewed to determine whether such a control is still warranted, and commodities that may be exported under general license to most destinations are examined to ascertain whether controls should be extended or expanded.[292]

Violations. Anyone who willfully violates or conspires to or attempts to violate any provision of the EEA with knowledge that the exports involved will be used for the benefit of, or that the destination or intended destination of the goods or technology involved is to, any controlled country or any country to which exports are controlled for national security or foreign policy purposes, shall be subject to penalties. Except in the case of an individual, the violator shall be fined not more than 5 times the value of the exports involved or $1,000,000, whichever is greater; or, in the case of an individual, the violator shall be fined not more than $250,000, or imprisoned not more than 10 years, or both.[293]

---

[285]. 15 C.F.R. § 770.3(a).

[286]. Table of Denial Orders Currently in Effect, 15 C.F.R. § 788, Supplement 1.

[287]. Definition of General License, 15 C.F.R. § 770.2.

[288]. 15 C.F.R. § 772.2(a).

[289]. For definitions see 15 C.F.R. § 772.2(b)(1)-(5).

[290]. 15 C.F.R. § 770.13(i)(1).

[291]. 15 C.F.R. § 770.13(j)(1)-(2).

[292]. 15 C.F.R. § 770.1(b)(1).

Any person who is issued a validated license under this Act for the export of any goods or technology to a controlled country and who, with knowledge that such goods or technology is being used by such controlled country for military or intelligence gathering purposes contrary to the conditions under which the license was issued, willfully fails to report such use to the Secretary of Defense shall be subject to penalties. Except in the case of an individual, a violator shall be fined not more than five times the value of the exports involved or $1,000,000, whichever is greater, or, in the case of an individual, shall be fined not more than $250,000, or imprisoned not more than 5 years, or both.[294]

Civil penalties may be enforced and may not exceed $500,000 for each violation. Civil penalties may be in addition to or in lieu of any other liability or penalty which may be imposed.[295]

2.2.2.2 Encryption technology on the Commerce Control List

Requirements for licenses of encryption technology appear in Category 5, Part II?Telecommunications, Information Security, in Supplement No. 1 of the CCL. All items with encryption capabilities that are controlled by the Commerce Department appear in this section. All encryption technology, with a few exceptions, require a validated license.[296]

Initially, all encryption technology appeared in the ITAR and was controlled by the State Department, but recent amendments moved some of these items to the CCL. Cryptographic items now controlled by the Commerce Department are those involving message authentication, access control devices, television descramblers, automatic teller machines, virus protection, and “smart cards.” Also, certain (but not all) types of mass-market software have been decontrolled by the State Department. Mass market software not decontrolled remains under the control of the State Department.[297]

2.2.3 Invention Secrecy Act, 35 U.S.C. §§ 181-188

The Invention Secrecy Act prevents the disclosure of patent applications filed in the Patent and Trademark Office for inventions made in the United States. Patent applications containing subject matter that may be detrimental to the national security if disclosed are subject to secrecy orders.

Regulations issued by the Patent and Trademark Office govern the export to foreign countries unclassified technical data in the form of a patent application or an amendment, modification, or supplement. These regulations are found under 37 C.F.R. part 5.

Secrecy orders. Patent applications containing subject matter that may be detrimental to national security interests if disclosed are made available for inspection by defense agencies.[298] If it is determined that the disclosure or publication of the invention by granting a patent would in fact be detrimental to the national security, the Commissioner, upon request from the defense agency, will

293. 50 U.S.C. App. § 2410(b)(1)(A)-(B).

294. 50 U.S.C. App. § 2410(b)(2)(A)-(B).

295. 50 U.S.C. App. § 2410(c).

296. See 15 C.F.R. § 799.1, Supp. 1, Cat. 5, pt. II, n.1-5.

297. See Interim Final Rule, amendments to ITAR, 57 Fed. Reg. 32148, July 20, 1992.

298. 37 C.F.R. § 5.1 (b).

issue an order that the invention be kept secret.[299] The secrecy order is directed to the subject matter of the patent application.[300] The secrecy order is enforced against the applicant, successors, any and all assignees, and any legal representatives.[301]

Petitions for rescission of secrecy order. A petition to rescind or remove a secrecy order may be filed by the applicant, assignees, or legal representatives.[302] The petition must include all facts that support a showing that the order is ineffectual or futile, or it may show where other applications not subject to a secrecy order disclose a significant part of the subject matter of the application under secrecy order.[303]

Petitions to export. Generally, if a secrecy order has been issued, an application cannot be exported to or filed in a foreign country.[304] However, a permit to disclose or modification of a secrecy order may be granted upon petition. The petition must fully recite the reason or purpose for the disclosure and all countries in which the petitioner wishes to file as well as all attorneys, agents, and others to whom the material will be consigned before filing in a foreign patent office.[305] The permit or modification may contain conditions and limitations on disclosure or filing.[306]

2.3 IMPORT CONTROLS

2.3.1 Temporary Imports (Intransit)

Items imported into the United States which may subsequently be reexported to another country are considered temporary imports. These items may be items that are intransit or merely passing through the United States from one country to another, or the item may be one that is sent to the United States for repairs, maintenance, etc. These items which are imported may be items that require export licenses from the State or Commerce Department. A temporary import license will allow the reexport of those items, even though such a license for a regular export may not be granted.

2.3.1.1 Import jurisdiction

The State Department regulates the temporary import of defense articles which appear on the U.S. Munitions List. Permanent imports of defense articles into the United States are regulated by the Treasury Department[307] (see 27 C.F.R. parts 47, 178, and 179).

2.3.1.2 Temporary import licenses

---

299. 37 C.F.R. § 5.2(a).
300. 37 C.F.R. § 5.2(d).
301. 37 C.F.R. § 5.2(b).
302. 37 C.F.R. § 5.4(a).
303. 37 C.F.R. § 5.4(b); 37 C.F.R. § 5.2(d).
304. 37 C.F.R. § 5.11(d).
305. 37 C.F.R. § 5.5(b),(c).
306. 37 C.F.R. § 5.5(e).
307. 22 C.F.R. § 123.2.

A temporary import license is required for the temporary import and subsequent export of unclassified defense articles, unless exempted in accordance with 22 C.F.R. 123.4. Licenses from the State Department are required for (1) temporary imports of unclassified defense articles that are to be returned directly to the country from which they were shipped to the United States, and (2) temporary imports of unclassified defense articles in transit to a third country.[308]

2.3.1.3 Encryption technology controls

The encryption devices that appear in Category XIII of the U.S. Munitions List are regulated by the State Department for temporary importation.

2.3.2 Permanent Imports

Items that are imported into the United States as a final destination for use or consumption are considered permanent imports. Typically, the Bureau of Alcohol, Tobacco and Firearms (Treasury Department) regulates the import of defense articles. The FCC also regulates a few items pertaining to communications. These two agencies may affect the import of encryption technology if the item falls within its jurisdiction.

2.3.2.1 Treasury Department, Bureau of Alcohol, Firearms and Tobacco controls

The Treasury Department regulates the permanent importation of defense articles which appear on the U.S. Munitions Import List.[309] This list was developed from the U.S. Munitions List, minus items not subject to controls. Category XIII, consisting of encryption technology, has been deleted from the U.S. Munitions Import List, and those items are not controlled by the Treasury Department.

2.3.2.2 Federal Communications Commission controls

Pursuant to the Communications Act, 47 U.S.C.S. § 302a, the FCC has regulations prohibiting the importation of scanning devices equipped with decoders that convert digital cellular transmissions to analog voice audio or scanning devices that may receive transmissions allocated to cellular radio telecommunications service. The control of the import of these items may involve items using encryption technology.

2.3.2.3 Commerce Department controls

Regulation. The Commerce Department will receive from the importers in the United States the representations regarding the intended destination of commodities.[310] An importer will certify to the exporting country that he will import specific commodities into the economy of the United States and will not reexport such commodities except in accordance with the export regulations of the United States.[311]

---

[308] 22 C.F.R. § 123.3(a)(1)-(2).

[309] 22 C.F.R. § 47.21.

[310] 15 C.F.R. § 768.1(a)(2)(i).

[311] 15 C.F.R. § 768.1(a)(1).

Violations and sanctions. A maximum fine of $10,000 or imprisonment for 5 years, or both, may be imposed for those making willfully false statements or concealing material fact or knowingly using a document containing a false statement in any matter.

3. BIBLIOGRAPHY

3.1 CITATIONS APPLICABLE TO THE FIRST AMENDMENT, FREEDOM OF SPEECH (Sect. 1.1.1)

3.1.1 Cases

1. *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

2. *Cable/Home Communication v. Network Productions*, 902 F.2d 829 (11th Cir. 1990).

3. *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of New York*, 447 U.S. 557 (1980).

4. *Consolidated Edison Co. of New York, Inc., v. Public Service Comm'n of New York*, 447 U.S. 530 (1980).

5. *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749 (1985).

6. *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978).

7. *First National Bank of Boston v. Bellotti*, 435 U.S. 765 (1978).

8. *Haig v. Agee*, 453 U.S. 280 (1981).

9. *Members of the City Council of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789 (1984).

10. *Near v. Minnesota ex rel. Olson*, 283 U.S. 716 (1931).

11. *New York Times v. United States*, 403 U.S. 713 (1971).

12. *Ohralik v. Ohio State Bar Association*, 436 U.S. 447, 456 (1978).

13. *Smith v. Gogen*, 415 U.S. 566 (1974).

14. *Steve Jackson Games, Inc. v. U.S. Secret Service*, 816 F.Supp. 432 (W.D. Tex. 1993).

15. *United States v. Donas-Botto*, 363 F.Supp. 191 (E.D. Mich. 1973).

16. *United States v. The Progressive, Inc.*, 467 F.Supp 990 (1979).

17. *United States v. Posey*, 864 F.2d 1487 (9th Cir. 1988).

18. *United States v. Van Hee*, 531 F.2d 352 (6th Cir. 1976).

19. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

20. *Village of Hoffman Estates v. The Flipside, Hoffman Estates*, 455 U.S. 489 (1982).

21. *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council Inc.*, 425 U.S. 748 (1976).

3.1.2 Law Review Articles

1. Emerson, *The Doctrine of Prior Restraint*, 20 Law & Contemporary Problems 648 (1955).

2. Ferguson, James R., *Scientific Inquiry and the First Amendment*, 64 Cornell L. Rev. 639 (1979).

3. Katsh, M. Ethan, *The First Amendment and Technological Change: The New Media Have a Message*, 57 Geo. Wash. L. Rev. 1459 (1989).

4. Funk, Roger, *National Security Controls on the Dissemination of Privately Generated Scientific Information*, 30 UCLA L. Rev. 405 (1982).

5. Shinn, Allen, Jr., *The First Amendment and the Export Laws: Free Speech on the Scientific and Technical Matters*, 58 Geo. Wash. L. Rev. 368 (1990).

6. Taviss, Michael L., *Dueling Forums: The Public Forum Doctrine's Failure to Protect the Electronic Forum*, 60 U. Cin. L. Rev. 757 (1992).

3.2 CITATIONS APPLICABLE TO EXPORT/IMPORT CONTROLS (Sect. 1.1.1.1)

1. *United States v. Elder Industries, Inc.*, 579 F.2d 516 (9th Cir. 1978) (cert. denied).

2. *United States v. Geissleer*, 731 F.Supp 93 (E.D. NY. 1990).

3. *United States v. Gregg*, 829 F.2d 1430 (8th Cir. 1987) (cert. denied).

3.3 CITATIONS APPLICABLE TO THE FIRST AMENDMENT, PRIVACY (Sect. 1.1.2)

3.3.1 Cases

1. *Department of Justice v. Reporter's Commission*, 489 U.S. 749 (1989).

2. *Griswold v. Connecticut*, 381 U.S. 479 (1965).

3. *Katz v. United States*, 389 U.S. 347 (1967).

4. *NAACP v. Alabama*, 357 U.S. 449 (1958).

5. *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977).

6. *Olmstead v. United States*, 277 U.S. 438 (1928).

7. *Paul v. Davis*, 242 U.S. 693 (1976).

8. *Roe v. Wade*, 410 U.S. 113 (1973).

9. *Stanley v. Georgia*, 394 U.S. 557 (1969).

10. *United States v. Skowronski*, 827 F.2d 1414 (1987).

11. *Whalen Commissioner of Health of New York v. Roe*, 429 U.S. 589 (1977).

3.3.2 Law Review Articles

1. Branscomb, Anne W., *A Special Symposium: The New Technology in the Communications Industry: Legal Problems in a Brave New World: Global Networks: A Survey of Transborder Data Flow in Transition*, 36 Vand. L. Rev. 985 (1983).

2. Coles, Todd Robert, *Symposium on the Selection and Function of the Modern Jury: Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 Am. U. L. Rev. 957 (1991).

3. Fein, Bruce E., *National Security and the First Amendment: Article: Access to Classified Information: Constitutional and Statutory Dimensions*, 26 Wm. & Mary L. Rev. 805 (1985).

4. Firehock, Gregory R., *Privacy Act: The Increased Invulnerability of Incorrect Records Maintained by Law Enforcement Agencies: Doe v. FBI*, 60 Geo. Wash. L. Rev. 1509 (1992).

5. Franks Renae A., *The National Security Agency and Its Interference with Private Sector Computer Security*, 72 Iowa L. Rev. 1015 (1987).

6. Note, *The Interest in Limited Disclosure of Personal Information: A Constitutional Analysis*, 36 Vand. L. Rev. 139 (1983).

7. Note, *The Unconstitutionality of Interference in Civilian Cryptography Under Present Procedures*, 22 Santa Clara L. Rev. 327 (1982).

3.3.3 Statutes

1. Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988). (Congressional Law)

2. Exec. Order No. 12356, 3 C.F.R. 166 (1983). (Administrative Law)

3. Privacy Act of 1974, 5 U.S.C. § 552(a), Pub. L. No. 93-579, 88 Stat. 1896 (1988). (Congressional Law)

3.4 CITATIONS APPLICABLE TO THE SECOND AMENDMENT (Sect. 1.2)

3.4.1 Cases

1.*Miller v. Texas*, 15 U.S. 5353 (1984).

2.*Presser v. Illinois*, 116 U.S. 252 (1886).

3.*U.S. v. Cruishank*, 92 U.S. 542 (1876).

4.*U.S. v. Miller*, 307 U.S. 174 (1939).

3.4.2 Law Review Article

1.Cottrol, Robert J., Raymond J. Diamond, *The Second Amendment: Toward an Afro-Americanist Reconsideration*, 80 Geo. L. J. 309 (1991).

3.5 CITATIONS APPLICABLE TO THE FOURTH AMENDMENT (Sect. 1.3)

3.5.1 Cases

1.*Berger v. New York*, 388 U.S. 41 (1966).

2.*Haklin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982).

3.*Katz v. United States*, 389 U.S. 347 (1967).

4.*Olmstead v. United States*, 277 U.S. 438 (1928).

5.*Osborn v. United States*, 385 U.S. 323 (1966).

6.*State v. Hemple*, 576 A.2d 793 (N.J. 1990).

7.*Steve Jackson Games, Inc. v. U.S. Secret Service*, 816 F.Supp. 432 (W.D. Tex. 1993).

8.*Terry v. Ohio*, 392 U.S. 1 (1968).

9.*United States v. Karo*, 486 U.S. 705 (1984).

10.*United States v. Leary*, 846 F.2d 592 (10th Cir. 1988).

11.*United States v. United States District Court*, 407 U.S. 297 (1972).

3.5.2 Law Review Articles

1.Birkenstock, Gregory E., *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 Geo. L. J. 843 (1992).

2.Cinquegrana Americo R., *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Pa. L. Rev. 793 (1989).

3.Hwang Kelley K., *The Admissibility of Evidence Obtained by Eavesdropping on Cordless Telephone Conversations*, 86 Colum. L. Rev. 323 (1986).

4.Note, *Computer Intellectual Property and Conceptual Severance*, 103 Harv. L. Rev. 1046 (1990).

5.Reetz C., *Warrant Requirement for Searches of Computerized Information*, 67 B. U. L. Rev. 179 (1987).

3.5.3 Statutes

1.Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 et seq. (Chapter 121?Stored Wire and Electronic Communications and Transactional Records Access), Pub. L. No. 100-690, 102 Stat. 4405 (1988). (Congressional Law)

2.Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 et seq., Pub. L. No. 95-511, 92 Stat. 1783 (1978). (Congressional Law)

3.Title III of the Omnibus Crime Control and Safe Street Act, 18 U.S.C. § 2510 et. seq. (Chapter 119?Wire and Electronic Communications Interception of Oral Communications), Pub.L. No. 99-508, 100 Stat. 1848, 1851 (1986). (Congressional Law)

3.6 CASES APPLICABLE TO THE FIFTH AMENDMENT (Sect. 1.4)

1.*Agnello v. United States*, 269 U.S. 20 (1925).

2.*Baltimore City Dept. of Social Serv. v Bouknight*, 493 U.S. 549 (1990).

3.*Berger v. New York*, 388 U.S. 41 (1967).

4.*Couch v. United States*, 409 U.S. 322 (1973).

5.*Doe v. United States*, 487 U.S. 201 (1988).

6.*Fisher v. United States*, 425 U.S. 391 (1976).

7.*Gouled v. United States*, 255 U.S. 298 (1921).

8.*In re Grand Jury Subpoena*, 487 F.2d 1172 ().

9.*Katz v. United States*, 389 U.S. 347 (1967).

10.*Osborn v United States*, 385 U.S. 323 (1966).

11.*United States v. Lefkowitz*, 285 U.S. 452 (1932).

12.*United States v. Doe*, 465 U.S. 605 ().

13.*Warden v. Hayden*, 387 U.S. 294 (1967).

3.7 CITATIONS APPLICABLE TO THE U.S. CONTROLS ON ENCRYPTION TECHNOLOGY (Chap. 2)

3.7.1 Statutes

1.Arms Export Control Act, 22 U.S.C.S. § 2778, Pub. L. No. 90-629.

2.40 U.S.C.S. § 759(a), Pub. L. No. 89-306, 79 Stat. 1127.

3.Communications Act, 47 U.S.C.S. § 302a, Pub. L. No. 90-379.

4.Computer Security Act, 40 U.S.C.S. § 759, Pub. L. No. 100-235, 101 Stat. 1724

5.Export Administration Act, 50 U.S.C.S. app. §§ 2401-2420, Pub. L. No. 96-72.

6.Invention Secrecy Act, 35 U.S.C.S. §§ 181-188, 66 Stat. 805.

3.7.2 Regulations

1.Export Administration Regulations, 15 C.F.R. pts. 768-799. Supplement No. 1 to § 799.1, Commerce Control List; Supplement No. 2 to § 799.1, General Software Note.

2.International Traffic in Arms Regulations (ITAR), 22 C.F.R. pts. 120-130. Final Rule, amendments to ITAR (57 Fed. Reg 15227, April 27, 1992); General?The U.S. Munitions List, 22 C.F.R. § 121.1. Interim Final Rule, amendments to ITAR (57 Fed. Reg. 32148, July 20, 1992); the U.S. Munitions List, 22 C.F.R. § 121.1, note added to Category XIII(b)(1). Final Rule, amendments to the ITAR (58 Fed. Reg. 39280, July 22, 1993).

3.Importation of Arms, Ammunitions and Implements of War, 27 C.F.R. pt. 47.

4.Secrecy of Certain Inventions and Licenses to Export and File, 37 C.F.R. pt. 5.

3.7.3 Law Review Articles

1.Franks, Renae Angeroth, *The National Security Agency and Its Interference with Private Sector Computer Security*, 72 Iowa L. Rev. 1015 (May 1987).

2.Pierce, Kenneth J., *Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation*, 17 Cornell Int'l L.J. 197 (1984).

3.Shinn, Allen M. Jr., *The First Amendment and the Export Laws: Free Speech On Scientific and Technical Matters*, 58 Geo. Wash. L. Rev. 368 (November 1989).

3.7.4 Other Publications

1.Browning, Graeme, *Software Hardball*, 24 Nat'l J. 2062, Sept. 12, 1992.

2.Groner, Jonathan, *U.S. Export Limits Split Software Makers, NSA; Sales vs. Cold War Mentality*, Legal Times, December 7, 1992, at 1.

3.Peterson, Ivars, *A Fierce Debate Erupts Over Cryptography and Privacy*, 143 Science News 394, June 19, 1993.

4.Rarog, Bob, *Statement by Bob Rarog, Export Policy Manager, Digital Equipment Corporation, to the Computer Systems Security and Privacy Advisory Board*, June 3, 1993.

5.Smoot, Ollie, *Statement of the Computer and Business Equipment Manufacturers Association (CBEMA)*, May 27, 1993.

6.Daily Report For Executives, 1991 DER 112 A9, *Export Controls, Restrictions Will Weaken Communications Security Technology, Conference Says*, June 11, 1991.

7.Daily Report For Executives, 1992 DER 140 d2, *Today's Summaries*, July 21, 1992.

8.Daily Report For Executives, 1992 DER 140 d5, *Export Controls, U.S. Sets Procedures for Easing Controls on Exports of Encoding-Capable Software*, July 21, 1992.

9.Daily Report For Executives, 1993 DER 82 d25, *Communications, Communications Policy Must Address Security, Fraud Issue*, April 30, 1993.

10.Daily Report For Executives, 1993 DER 88 d22, *Communications, Group Calls For Attention to Network Privacy in Administration Policy Review*, May 10, 1993.

11.Daily Report For Executives, 1993 DER 105 d22, *Communications, Commerce Advisory Board Faces Doubts About `Clipper Chip' Initiative*, June 3, 1993.

12.Daily Report For Executives, 1993 DER 106 d27, *Communications, Industry Criticizes `Clipper Chip'; Calls for Review of Other Systems*, June 4, 1993.

13.Daily Report For Executives, 1993 DER 107 d23, *Communications, Further Review Needed For Clipper Chip, Says Commerce Department Advisory Board*, June 7, 1993.

14.Daily Report For Executives, 1993 DER 110 d24, *Communications, House Subcommittee Skeptical of Proposed Communications Coding Device*, June 10, 1993.
K/DSRD/SUB/93-RF105/2
Limited Distribution

INTERNAL DISTRIBUTION

1. J. P. Chandler
2. L. J. Hoffman
3. K. D. Streetman
4-8. National Institute of Standards and Technology
9. DSRD Resource Center, 1099 COM, MS 7615, Room 507
10. K-25 Site Records, K-1001, MS 7101?RC