BERNSTEIN, *KARN*, AND *JUNGER*: CONSTITUTIONAL CHALLENGES TO CRYPTOGRAPHIC REGULATIONS

I. INTRODUCTION

Our Founding Fathers penned the First Amendment over two hundred years ago, and its speech protections are applicable today to regulations of electronic speech. Although technology has radically changed since 1791, the Speech Clause has always kept pace with new technology and the free exchange of ideas and information. It is fitting that as we approach the twenty-first century—an era denoted as the Information Age—that the First Amendment be given the opportunity to flex its muscles with regard to the Internet.

The Internet is a vast wealth of ideas and expression which draws its strength from its diversity. The Internet allows people from across the globe to come together to do business, debate worldly events, and share discoveries without regard to distances or borders. The accessibility of cyberspace has enabled more people to take active roles in communication because of the ease in placing information at the fingertips of others. Thus, people have become active producers and publishers of information on practically any topic imaginable. From politics to pole vaulting, and barbecue to bass fishing, information is only one point-and-click away.

Although technology has opened new First Amendment doors to promote free speech, it has also created new privacy concerns. Because much of today's electronic communication occurs in the form of e-mail, modern technology allows those messages to be tracked and stored by unintended recipients—namely the government. In addition, as more commerce takes place online, vital information about personal financial condition or personal tastes and preferences may become available to anyone with the motive to take advantage of the unsuspecting. To prevent Internet communication and commerce from becoming no more private than mailing a post card, technology has yet again delivered an answer.

Encryption technologies serve as the locks and keys of cyberspace. Cryptography has created new opportunities to protect our private communications and intimate information so that this electronic medium can continue to grow. Industry and commerce can prosper with the assurance that information and trade secrets can be transferred electronically with security. However, the increasing popularity of encryption technology has raised the ire of the government in the name of national security. In an effort to control the rapid growth of cryptography, the government has enacted laws controlling cryptography's development and dissemination. The laws have the effect of inhibiting the free flow of ideas among people who wish to communicate in this manner. The existing laws remove an entire area of communication from public debate and pose the potential to bar the First Amendment from electronic communication.

This Article focuses on the constitutional issues surrounding the development of cryptographic technology and suggests that existing regulations fail to pass constitutional muster. Three cases have arisen in the federal courts challenging governmental restrictions on the development and dissemination of cryptography, and the courts have taken contrasting views of the First Amendment issues involved.[1] Because of the importance of these issues and the potential effects of divergent rulings in lower courts, the Supreme Court may have to make the final decision. This Article asserts that if this issue reaches the Supreme Court, the Court should find the cryptographic regulations to be an unconstitutional suppression of free speech. Moreover, this Article proposes that the current regulations be stricken in favor of pending legislation before Congress.

Part II of this Article offers a basic introduction to the subject of cryptography and its uses. Part III analyzes the individual cases of Daniel Bernstein, Phillip Karn, and Peter Junger and the procedural history of their respective cases. Part IV discusses the constitutional flaws of the existing regulations in refer-

1. Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998); Karn v. United States Dep't of State, 925 F. Supp. 1 (D.D.C. 1996); Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996), *motions for summary judgment granted in part and denied in part*, 945 F. Supp. 1279 (N.D. Cal. 1996), *cross motions for summary judgment granted in part and denied in part*, 974 F. Supp. 1288 (N.D. Cal. 1997).

ence to the First, Fourth, and Fifth Amendments to the Constitution. Part V discusses alternative proposals to the existing encryption regulations including congressional attempts to legislate a superior solution to the current situation. Part VI concludes the Article with a look toward the future.

II. INTRODUCTION TO CRYPTOGRAPHY

A. What Is Cryptography?

Cryptography is the art of creating and using methods of disguising messages, using codes, ciphers, and other methods, so that only certain people can see the real message.[2] The process of disguising the substance of messages into incomprehensible data is called encryption.[3] The encryption process converts the undisguised message, or plaintext, into unintelligible ciphertext.[4] After the message has been encrypted, it may be transformed back to plaintext in a process called decryption.[5] The tool which performs the conversion is a cipher, which is a method of encryption that utilizes a mathematical algorithm to convert any text regardless of its content.[6] As an added level of security, today's algorithms use a key which consists of a sequence of computer code to activate the algorithm to encrypt and decrypt messages.[7] The key is input into the algorithm to successfully perform the desired conversion.[8]

The strength of a coded communication is greatly dependent upon the key, for the algorithm itself is worthless without the key to decrypt the message.[9] Early encryption techniques em-

---

2. A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 713 (1995).

3. Jason Kerben, Comment, *The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Genie*, 5 COMMLAW CONSPECTUS 125, 125 (1997).

4. Laura M. Pilkington, *First and Fifth Amendment Challenges to Export Controls on Encryption:* Bernstein *and* Karn, 37 SANTA CLARA L. REV. 159, 168 (1996).

5. Kerben, *supra* note 3, at 125.

6. Pilkington, *supra* note 4, at 168.

7. Froomkin, *supra* note 2, at 714.

8. Lance J. Hoffman et al., *Cryptography: Policy and Technology Trends* (visited Apr. 19, 1999) <http://www.eff.org/pub/Privacy/crypto-policy_doe_94.report>.

9. Pilkington, *supra* note 4, at 168.

ployed a single key system that was required to both encrypt and decrypt the message.[10] This type of system was vulnerable because a separate key was needed for each pair of users who exchanged messages, and both sides had to keep the key secret to keep the system secure.[11]

In the mid 1980s, a more secure key system was developed to solve the single key exchange problem. The system of public key cryptography was created to utilize a public and a private key to encrypt and decrypt messages. Under this scheme, each party establishes a unique private key which only the owner knows and a unique public key which everyone knows.[12] Public keys may be published freely in directories similar to phone books to aid senders in locating a potential recipient's public key, but private keys must be kept secret by their owner.[13] Consider the following example:

> Sam completes a message to Ruth in plaintext form. Upon completion, Sam encodes the message with Ruth's public key. When Ruth receives the message in ciphertext from Sam, she uses her private key to decode the message into plaintext. To send a message back to Sam, Ruth encodes her message with the use of Sam's public key. Sam then uses his private key to decode the message.[14]

Ruth and Sam have not compromised their private keys. Knowledge of the public key in no way compromises the identity of the private key.[15] The system is extremely secure, as virtually the only way to break security is for either Ruth or Sam to give away their private keys. Public key cryptographic technology has delivered military-grade cryptography with the level of security so high that even the ultra-secret, code-breaking computers at the National Security Agency cannot decipher the encrypted messages.[16]

---

10. *Id.* at 169.
11. *Id.*
12. Kerben, *supra* note 3, at 128.
13. Pilkington, *supra* note 4, at 169.
14. Kerben, *supra* note 3, at 128.
15. *Id.*
16. Ronald J. Stay, Note and Comment, *Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann*, 13 GA. ST. U. L. REV. 581, 585 (1997).

B. Who Uses Cryptography?

One of the earliest examples of cryptography was used by Julius Caesar when he sent military messages to his armies.[17] Perhaps since that time, people have also tried to decode encrypted messages. Allies in World War II were able to break a secret German code called Enigma.[18] This discovery enabled Allied forces to locate and sink many German U-boats; moreover, they were able to obtain advanced information about German military operations that was critical to the campaign in Europe.[19] Similar code-breaking ability also allowed the United States Navy to intercept the Japanese fleet in one of the most decisive battles in the Pacific—The Battle of Midway.[20] These are just a few examples of how cryptographic technology has played an important role in history.

Until recently, cryptography has primarily been the vital and exclusive tool of governments, not the public; however, a demand for private encryption technology has arisen with the growth of advanced computer technology.[21] Today, many individuals and businesses want or need secure communications. For example, encryption is heavily used in the banking industry to ensure the security of electronic fund transfers.[22] In 1994, an international group of criminals attempted to electronically steal twelve million dollars from Citicorp.[23] As a result of the attempted heist, financial institutions around the world increased their authentication capabilities for electronic fund transfers.[24] Banks also encrypt ATM customer identification numbers and the data on the cards to prevent unauthorized modification and forgery.[25] As targets of industrial espionage, many U.S. corporations seek to secure communications to protect their intellectu-

---

17. Kerben, *supra* note 3, at 125.
18. Thinh Nguyen, *Cryptography, Export Controls, and the First Amendment in* Bernstein v. United States Department of State, 10 HARV. J.L. & TECH. 667, 668 (1997).
19. *Id.*
20. *Id.*
21. *See id.*
22. *See* Pilkington, *supra* note 4, at 162.
23. Nguyen, *supra* note 18, at 670.
24. *Id.*
25. Froomkin, *supra* note 2, at 720.

al property and other sensitive market information.[26] Exponential growth in the Internet and the popularity of e-mail have given rise to encryption needs.[27] Because cryptography can deliver secure transactions and communications on an unsecure worldwide computer network, the technology is essential to the commercial expansion of the Internet.[28]

C. The Government's View of Cryptography

Because the early uses of cryptography were primarily for intelligence gathering and securing military communications, the Defense Department, through the National Security Agency (NSA), has played a key role in developing the science and controlling its use in the United States and abroad.[29] The NSA has continuously attempted to control the development and expansion of cryptography in the private sector because it views the technology as a threat to national security.[30] The NSA has tried to slow the growth and dissemination of cryptography by controlling public funding, patent publications, and presentation of scientific papers at academic conferences.[31] To accomplish the NSA's task, the government has enacted export control laws to restrict the exportation and dissemination of encryption software.

One of the first laws enacted to regulate cryptography authorized the President, under the Arms Export Control Act (AECA), to control the export and import of defense articles and services by designating them as munitions on the United States Munitions List (USML).[32] Regulatory responsibility for the AECA was vested in the Department of State, which instituted the International Traffic in Arms Regulations (ITAR) for admin-

---

26. *Id.* at 722-23.

27. *Id.*

28. Encryption could help producers receive authenticated orders from consumers to the extent that one day Internet consumer business could exceed catalog shopping. *See* Kerben, *supra* note 3, at 139.

29. Pilkington, *supra* note 4, at 162.

30. *Id.*

31. *Id.*

32. International Security Assistance and Arms Export Control Act of 1976, Pub. L. No. 90-629, 90 Stat. 744 (codified at 22 U.S.C.A. §§ 2778-2796 (West 1990 & Supp. 1998)).

istration of this task.[33]

Once an item is placed on the USML, it must be licensed before it can be imported or exported.[34] Requests to license items listed on the USML are made to the Office of Defense Trade Controls (ODTC), which considers requests on a case-by-case-basis.[35] The ITAR provides for a commodity jurisdiction procedure allowing the ODTC to determine whether an article or service is covered by the USML.[36] If an article is not listed on the USML, then it can be freely exported.

The USML's scope includes articles such as "military tanks, combat engineer vehicles, bridge launching vehicles, half-tracks and gun carriers."[37] The USML also considers encryption technology as a "munition" having been "specifically designed, developed, configured, adapted, or modified for a military application . . . ."[38] Cryptographic software is covered by Category XIII(b)(1) of the USML.[39] If the ODTC determines that a license is required for a cryptographic item covered by the USML, the petitioning party must comply.[40] A violator of a license or order of the ITAR under the AECA is subject to a $1,000,000 fine with the possibility of imprisonment for not more than ten years.[41]

The ITAR is not the only law controlling the development and dissemination of cryptography. In November 1996, President Clinton by Executive Order transferred jurisdiction over the export of nonmilitary encryption products to the Department of Commerce.[42] The order removed encryption products that would qualify as defense articles under the USML and placed them on the Commerce Control List under the authority of the

---

33. 22 C.F.R. §§ 120-30 (1998).
34. 22 U.S.C. § 2778(b)(2) (1994).
35. 22 U.S.C.A. § 2778(a)(2) (West Supp. 1998).
36. 22 C.F.R. § 120.4(a) (1998).
37. *Id.* § 121.1 Category VII(b).
38. *Id.* § 120.3(a).
39. This category includes "[m]ilitary cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems . . . ." *Id.* § 121.1 Category XIII(b)(1).
40. *Id.* § 120.4(b).
41. 22 U.S.C. § 2778(c) (1994).
42. Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996).

Export Administration Regulations (EAR).[43]

Shortly after the President signed the order, the Commerce Department issued an interim rule regulating the export of encryption products. The Commerce Department declared that encryption items include all "encryption commodities, software, and technology that contain encryption features and are subject to the EAR."[44] The EAR considers export as the downloading, or causing the downloading of software through Internet file transfer protocol locations, to bulletin boards, and on World Wide Web sites.[45] To disseminate information subject to the EAR, one must obtain a license prior to any transmission.[46] Both civil and criminal sanctions are possible for violating any order or license of the EAR, ranging up to a $250,000 fine and imprisonment up to ten years.[47]

Even with the EAR, encryption products with military application remain under the power of the ITAR.[48] Because both the ITAR and EAR have control over cryptography, it is necessary to examine the constitutional ramifications of each to discover potential problems in the two laws.

III. PRESENT LITIGATION

A. *The* Bernstein *Case*

In 1992, Daniel Bernstein was a graduate student in mathematics at the University of California at Berkeley. He wrote an encryption algorithm called "Snuffle" while conducting his graduate research. Bernstein wanted to publish his work, present his technical paper at academic conferences, and teach the algorithm in his classes. Concerned about potential criminal liability, Bernstein submitted a commodity jurisdiction request to the State Department to determine whether the computer program

43. *Id.* The EAR derives its authority from the Export Administration Act of 1979. 50 U.S.C.A. app. § 2401 (West 1997).

44. 15 C.F.R. § 772 (1998).

45. Bernstein v. United States Dep't of State, 974 F. Supp. 1288, 1295 (N.D. Cal. 1997).

46. 15 C.F.R. § 740.1 (1998).

47. *Id.* § 764.3.

48. *Bernstein*, 974 F. Supp. at 1291.

and his academic paper were controlled by ITAR.[49] The ODTC later informed Bernstein that the computer program was a defense article and was subject to licensing by the Department of State prior to export.

Because Bernstein was not allowed to teach the mathematical algorithm, to present the accompanying academic paper at scholarly conferences, or to publish the article in periodicals without first obtaining a license from the government, he filed suit in the District Court for the Northern District of California seeking declaratory and injunctive relief against the Department of State to prevent it from enforcing the AECA.[50] After the partial shift in control over cryptography to the Commerce Department in Executive Order 13,026, Bernstein amended his complaint to include the EAR.[51]

In holding that cryptographic computer code is speech, the district court in *Bernstein v. United States Department of State*[52] became the first court to recognize a protected speech interest in computer source code.[53] In denying the government's motion to dismiss for lack of justiciability, the court found that Bernstein did assert a "colorable" constitutional claim.[54] The court stated that Bernstein's academic writing explaining his scientific work in the field of cryptography is speech of the most protected kind.[55] With regard to the source code, the court resoundingly rejected the notion that a computer program is expressive conduct by stating that it is totally "unlike flag burning and nude dancing."[56] Judge Patel reasoned that even though source code has functional qualities in that it is compiled into object code for the computer to read and execute, computer programming code is no different from instructions, do-it-yourself manuals, or recipes that are purely functional, but yet also recognized as speech.[57] Thus, the court found "no meaningful dif-

---

49. Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1430 (N.D. Cal. 1996).
50. *Bernstein*, 922 F. Supp. at 1428.
51. *Bernstein*, 974 F. Supp. at 1292.
52. 922 F. Supp. 1426 (N.D. Cal. 1996).
53. Nguyen, *supra* note 18, at 672.
54. *Bernstein*, 922 F. Supp. at 1432-34.
55. *Id.* at 1434 (citing Sweezy v. New Hampshire, 354 U.S. 234, 248 (1957)).
56. *Id.* at 1435.
57. *Id.*

ference between computer language, particularly high-level languages . . . and German or French" and reasoned that the source code "operates as a 'language'" capable of communicating expressible ideas.[58] With that finding, the district court concluded that computer source code is speech.[59]

Judge Patel also held that the licensing requirements for speech relating to encryption of computer software constituted an unlawful prior restraint.[60] The regulations conditioned speech on obtaining a license or permit from a government official in that official's boundless discretion.[61] Because the prior restraint froze speech as a result of the licensing requirements and process, it was an unconstitutional abridgment of the First Amendment.[62]

B. The Karn *Case*

In 1994, Phillip Karn submitted a commodity jurisdiction request to the Department of State as an exporter of a book written by his good friend Bruce Schneier entitled *Applied Cryptography*.[63] The book contained information on cryptographic protocols, algorithms, techniques, and applications, and it included examples of source code for several cryptographic algorithms. The ODTC determined that the book was not subject to the jurisdiction of the State Department under the ITAR.[64] The ODTC's decision allowed the book to be sold in the United States and abroad.[65]

---

58. *Id.* at 1435.

59. *Bernstein*, 922 F. Supp. at 1436.

60. Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1290 (N.D. Cal. 1996) (relying largely on FW/PBS, Inc. v. Dallas, 493 U.S. 215 (1990); Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984); Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976); New York Times Co. v. United States, 403 U.S. 713, 714 (1971); Freedman v. Maryland, 380 U.S. 51, 58 (1965); Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 713 (1931)).

61. *Bernstein*, 945 F. Supp. at 1286.

62. *See id.*

63. Actually, Karn was interested in exporting the book and the disk version of the source code contained in the book even though he was not the author because he wanted to test the existing laws and show how silly they were. Kerben, *supra* note 3, at 152 n.185.

64. Karn v. United States Dep't of State, 925 F. Supp. 1, 3 (D.D.C. 1996).

65. Within about the first year of the book's release, approximately 25,000 cop-

Shortly after receiving approval to export the book, Karn submitted another commodity jurisdiction application, this time for the export of a floppy disk of the book, which contained a verbatim copy of the source code depicted in the book. This time, the ODTC decided that the computer disk was subject to the jurisdiction of the Department of State pursuant to the ITAR as a defense article.[66] Subsequent appeals within the Department of State were denied.[67] As a result, Karn was required to obtain an export license for the information contained on the floppy disk, but was free to export the same information in the medium of the book.

Karn brought suit against the Department of State claiming that the regulations on the diskette were a restraint on free speech in that the diskette should be considered "speech" for First Amendment purposes in order to allow dissemination and exportation.[68] Because the license requirement kept him from exporting the disk and its contents, Karn argued that his right to free speech was restricted.[69] Karn further argued that the content-neutral test articulated in *United States v. O'Brien*[70] should not apply, and in the alternative asserted that the test was not satisfied.[71] Finally, Karn contended that the ITAR constituted an unconstitutional system of prior restraint.[72]

In *Karn v. United States Department of State*,[73] the United States District Court for the District of Columbia took a completely different approach to and reached an opposite result from *Bernstein*. The court disagreed with the notion that the cryptographic source was "pure speech" and found it "unnecessary . . . to make any findings regarding the nature of the matter con-

---

ies were sold. Kerben, *supra* note 3, at 128.

66. *Karn*, 925 F. Supp. at 4.

67. *Id.* at 3.

68. *Id.* at 9.

69. *See id.*

70. 391 U.S. 367 (1968). The content-neutral test requires that the regulation be within the power of the government, further an important or substantial governmental interest, be unrelated to the suppression of free expression, and impose no greater a restriction than is essential to further the governmental interest. *O'Brien*, 391 U.S. at 377.

71. *See Karn*, 925 F. Supp. at 10-11.

72. *See id.* at 12.

73. 925 F. Supp. 1 (D.D.C. 1996).

tained on the Karn diskette."[74] Clearly, in the mind of the court, the regulations of the ITAR were content-neutral, so it utilized the *United States v. O'Brien* test.[75] Judge Richey deferred to the President's policy judgment and refused to scrutinize the decision to control the export of cryptographic products.[76] Thus, the ITAR was found to be justified under the *O'Brien* test.

Judge Richey further refused to find that the regulations were unconstitutional prior restraints on speech, but rather found that Karn lacked standing because he was not subjected to the provisions of the ITAR from which he sought relief.[77] For these reasons, the court granted the Defendant's motion for summary judgment on the First Amendment claims.[78]

C. *The* Junger *Case*

Law Professor Peter Junger teaches a course entitled "Computers and the Law" at Case Western Reserve University Law School in Cleveland, Ohio, and he maintains a web site containing information about his classes and interests.[79] He utilizes the web site to publish class materials and articles for his course in order to teach students how computers operate and how the law should be applied to computers.[80] Junger wanted to publish on his web site various encryption programs that he had written to demonstrate how computers function.[81] He therefore submit-

---

74. *Karn*, 925 F. Supp. at 10.

75. *Id.*

76. *Id.* at 11.

77. *Id.* at 12 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 559-61 (1992)).

78. *Id.* at 14.

79. Junger v. Daley, 8 F. Supp. 2d 708, 713 (N.D. Ohio 1998). Junger's web site can be found at http://samsara.law.cwru.edu/.

80. Peter Junger, *Federal District Court Holds That Software Publishers Are Not Protected by the First Amendment* (visited Apr. 19, 1999) <http://samsara.law.cwru.edu/comp_law/jvd/pressrel-070798.txt>.

81. *Junger*, 8 F. Supp. 2d at 714. In the course, Junger has used a short "one-time pad" (OTP) encryption program, which he initially wrote in May 1993, to demonstrate how computers work and how computer software is, or should be, covered by intellectual property law. Plaintiff's Supplemental and Amended Complaint at 6, Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998) (96-CV-1723). The plaintiff believed that his OTP program was subject to control under the EAR because he used it to encrypt and decrypt messages. *Id.*

ted three applications for thirteen items to the Commerce Department requesting classification for the encryption programs.[82] The government responded that four of the five programs submitted were subject to the Export Regulations and would need a license before he could publish them on his web site.[83]

Soon thereafter, Junger filed suit to enjoin the Commerce Department from enforcing the EAR against him.[84] Junger's complaint alleged that the encryption regulations violated his freedom of speech and press that are protected from prior restraints by the First Amendment.[85] Junger reasoned that because the Supreme Court extended First Amendment protection to pornographers in *Reno v. ACLU*, then computer programmers should at least be entitled to the same level of protection.[86]

In *Junger v. Daley*, yet another district court weighed in on its opinion of the constitutionality of the encryption regulations.[87] District Judge Gwin, writing for the Eastern Division of the Northern District Court of Ohio, concluded that computer programs are not constitutionally protected writings because they are "inherently functional" without any expressive content containing any "exposition of ideas."[88] Judge Gwin's distinction rested on the assertion that encryption source code is functional because "it is designed to *enable* a computer to do a designated task."[89] Judge Gwin held that encryption software does not communicate ideas such as explaining cryptographic theory or describing how the software functions; consequently, he reasoned that the value of encryption source code only comes from

---

82. *See Junger*, 8 F. Supp. 2d at 714.

83. *See id.* However, the Export Administration concluded that the first chapter of Junger's textbook on the subject was an allowed unlicensed export even though it contained printed encryption code as contained in the software program. *See id.*

84. Peter Junger, Press Release, *New Complaint Filed in Suit Challenging Constitutionality of Regulations Forbidding Publication of Software on Internet* (visited Apr. 19, 1999) <http://samsara.law.cwru.edu/comp_law/jvd/pr.txt>. Junger never applied for an export license because he believed that his license request would be denied. *See Junger*, 8 F. Supp. 2d at 714.

85. *Junger*, 8 F. Supp. 2d at 711. Junger's Complaint also claimed that the ITAR and EAR were unconstitutionally vague and overbroad. *Id.*

86. Junger, *supra* note 84.

87. 8 F. Supp. 2d 708 (N.D. Ohio 1998).

88. *Junger*, 8 F. Supp. 2d at 716.

89. *Id.* (emphasis added).

the function that the source code accomplishes.[90] While Judge Gwin recognized that certain types of software are inherently expressive for the ideas that are conveyed, he exempted encryption software from this list because it only carries out the function of encryption.[91]

Judge Gwin's analysis of the relationship between source code's inherent functionality and First Amendment protection was then compared to Judge Patel's *Bernstein* decision.[92] Judge Gwin attacked *Berstein's* holding that "language equals protected speech" as being totally unsound.[93] Judge Gwin asserted that speech is not protected just because it is written in a language, but the decisive factor is whether it expresses ideas.[94] Judge Gwin characterized *Bernstein's* holding—that encryption source code is similar to a set of instructions, do-it-yourself manuals or even recipes—as incorrect because the source code actually performs the function it describes.[95] Judge Gwin's distinction likened the encryption source code to embedded circuitry in a telephone even though it is composed of a set of characters that formulate commands.[96] Judge Gwin acknowledged that some people, such as computer programmers, are able to communicate and express ideas in source code language, but he denied First Amendment protection to conduct that is occasionally expressive.[97] As a result, Judge Gwin held that the export

---

90. *See id.*

91. *See id.* Judge Gwin failed to offer any examples of how expressive software operates without accomplishing a single designated task in the computer on which the software runs. The reason is that no such software exists. Almost by definition, all software has functional aspects because it makes the black boxes known as computers do something.

92. *Id.*

93. *Junger*, 8 F. Supp. 2d at 716.

94. *Id.* Judge Gwin pointed out that fighting words can be written or spoken in a language, but "they are excluded from First Amendment protection." *Id.* at 716-17.

95. *Id.* at 717.

96. *Id.*

97. *See Junger*, 8 F. Supp. 2d at 717. Judge Gwin reasoned that "[i]t is possible to find some kernel of expression in almost every activity . . . but such a kernel is not sufficient to bring the activity within the protection of the First Amendment." *Id.* (citing City of Dallas v. Stanglin, 490 U.S. 19, 25 (1989)). Judge Gwin cited *Texas v. Johnson*, 491 U.S. 397 (1989), *Spence v. Washington*, 418 U.S. 405 (1974), and *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969) to support his assertion that encryption source code is not sufficiently communicative. *See id.* This Article relies on these cases as examples of expressive con-

of encryption source code is not protected conduct under the First Amendment.[98]

Judge Gwin also rejected Junger's contention that the Export Regulations are invalid on their face as an unconstitutional prior restraint on the export of encryption source code because, as discussed above, the encryption software has little expressive value.[99] Because Judge Gwin opined that encryption source code is not an activity "commonly associated with expression," even though it may occasionally be expressive, he held that the prior restraint doctrine is not implicated.[100]

Judge Gwin also held that the Export Regulations do not discriminate against encryption software on the basis of content, so he rejected Junger's invitation to review the EAR under a strict scrutiny standard.[101] Instead, Judge Gwin held that the Export Regulations are not content-based because "the regulations burden encryption software without reference to any views it may express."[102] In Judge Gwin's opinion, the Export Regulations do not attempt to restrict the free flow of information and ideas about the subject of cryptography; therefore, they cannot be directed to the content of ideas.[103] Furthermore, Judge Gwin held that the regulations are not content-based because the EAR does not control export of publications on cryptography.[104] In rejecting strict scrutiny as the applicable standard, Judge Gwin instead opted for intermediate scrutiny and

---

duct protected by the First Amendment. *See infra* text accompanying notes 110-23.

98. *See Junger*, 8 F. Supp. 2d at 718.

99. *See id.*

100. *Id.* (citing City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 760 (1988)).

101. *Id.* at 720.

102. *Id.* Judge Gwin cited President Clinton's reason for the regulations as those related to national security interests. *See Junger*, 8 F. Supp. 2d at 720.

103. *See id.* Of course, the Export Regulations do not prohibit free discussion about the *topic* of cryptography, but that is not the issue. Bernstein, Karn, Junger, and others already engage in discussion about the topic of cryptography, but the Export Regulations prohibit them from sharing knowledge on the topic through specific examples. If Judge Gwin's reasoning were applied to the subject of cooking, the result would be that discussion about baking brownies would be allowed, but the sharing of the recipe and its ingredients would not.

104. *Id.* The problem with this line of reasoning is that printed encryption source code is equally as operable because today's computers are capable of running source code read from an optical scanning device.

held that the EAR satisfies this standard.[105]

IV. CONSTITUTIONAL ISSUES

A. The First Amendment

In an attempt to communicate their ideas and findings on cryptography to others, Bernstein, Karn and Junger sought and were denied free dissemination of their source code. However, only the district court in *Bernstein* held that the source code software was speech and thus protected by the First Amendment.[106]

The First Amendment to the United States Constitution states that "Congress shall make no law . . . abridging the freedom of speech."[107] The First Amendment protects a very broad range of expression, both artistic and scientific. However, the government believes that cryptographic algorithms are non-deserving of this protection.[108] The government seemingly fails to realize that to gain First Amendment protection, expression only has to be a vehicle or method for communication of thoughts, ideas, opinions, or emotions.[109]

Source code must fit into one of these vehicles of communication to be protected speech, and that is exactly what Bernstein, Karn and Junger argued. The government, however, argued that the enforcement laws regulate only conduct and not speech. Thus, a closer inspection must be made to determine whether computer source code is, in fact, speech or conduct, and what, if any, First Amendment protection applies.

The Supreme Court has stated that "[t]he First Amendment literally forbids the abridgment only of 'speech,' but [the Court has] long recognized that its protection does not end at the spo-

---

105. *Id.* at 722.

106. *See* Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1434-37 (N.D. Cal. 1996).

107. U.S. CONST. amend. I.

108. *See Bernstein*, 922 F. Supp. at 1429-38.

109. *See generally* Spence v. Washington, 418 U.S. 405 (1974) (determining that a flag misuse statute was unconstitutional in preventing expression of opinion); Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503 (1969) (holding that wearing black armbands in disapproval of Vietnam War was expression of opinion).

ken or written word."[110] In fact, the Court has extended First Amendment protection to expression which occurs in a novel or unfamiliar form.[111] For example, in *Tinker v. Des Moines Independent Community School District*,[112] the Court found a regulation prohibiting the wearing of armbands to schools in protest of Vietnam to be an unconstitutional denial of the right of expression of opinion.[113] The students wore the armbands on their sleeves to school, but were suspended from school under a policy adopted two days before their protest.[114] The Court found the actions were totally divorced from disruptive conduct, but were rather "pure speech."[115] It noted that the rights of the First Amendment cannot be confined to a telephone booth or to the four corners of a pamphlet, or to the supervised and ordained discussion in a school classroom.[116]

In *Spence v. State of Washington*,[117] the Court held that a flag misuse statute was unconstitutional as applied to a college student who hung a privately owned United States flag upside-down with a peace symbol affixed to it out of a window to express that America stood for peace.[118] The flag was displayed at the time of the Cambodian invasion and Kent State shootings. Police officers entered the student's apartment, seized the flag, and arrested him on the charge specified by the "improper use" statute.[119] In holding the statute unconstitutional, the Court found the expression to be speech because the symbol in its context—a plea for peace in the midst of war—was used for the purpose of expression, and thus was "symbolic speech."[120]

The Court extended First Amendment protection to expressive conduct exemplified by the burning of an American flag in *Texas v. Johnson*.[121] Johnson burned the flag during a political

110. Texas v. Johnson, 491 U.S. 397, 404 (1989).
111. *See Tinker*, 393 U.S. at 506.
112. 393 U.S. 503 (1969).
113. *Tinker*, 393 U.S. at 505.
114. *Id.* at 504.
115. *Id.* at 505.
116. *Id.* at 513.
117. 418 U.S. 405 (1974).
118. *Spence*, 418 U.S. at 414.
119. *Id.* at 406.
120. *Id.* at 410, 414.
121. 491 U.S. 397 (1989).

demonstration against the Republican party during the 1984 Republican National Convention and was convicted of desecration of a venerated object in violation of a Texas statute.[122] The Court reasoned that even nonverbal conduct can be expressive when the intent to convey a particularized message is present, and it is likely that the message will be understood by those who view it.[123] Thus, Johnson's actions were found to be protected by the First Amendment.

As these cases illustrate, the First Amendment's protection encompasses more than the literal word "speech." If the Court had interpreted speech to mean only those forms of communication known to the Framers of the Constitution at that time, many of today's vehicles which facilitate the free flow of ideas would not enjoy the level of First Amendment protection they do. As technological advances have taken communicative speech to new realms that were unfathomable when our country was founded, the Court has made sure that the First Amendment retains its fundamental power.

More recently, the Court in *Reno v. ACLU*[124] again embraced this idea in recognizing that digital information as manifested in the Internet is entitled to the broadest First Amendment protection possible. The Court stated that content on the Internet is as diverse as human thought and regulating potentially indecent material creates an obvious chilling effect on speech.[125] Such regulation places an "unacceptably heavy burden on protected speech" that "threatens to torch a large segment of the Internet community."[126] Thus, "[t]he interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship."[127] In so ruling, the Court suggested not only that the distinction between print and electronic media is increasingly untenable, but also that the Internet is subject to the same exacting First Amendment scrutiny as print media.[128]

---

122. *Johnson*, 491 U.S. at 399.
123. *See id.* at 404, 417.
124. 521 U.S. 844 (1997).
125. *See ACLU*, 521 U.S. at 852, 868-70.
126. *Id.* at 882.
127. *Id.* at 885.
128. *Id.* at 868-70.

The conclusion remains that speech in any language consists of the "expressive conduct" of vibrating one's vocal chords, moving one's mouth and thereby making sounds, or of putting hand to keyboard.[129] Yet the fact that such "conduct" is shaped by language—a sophisticated and complex system of understood meanings—is what makes it speech.[130] "[T]o ignore the substance of speech and to look solely to form . . . is to be wholly mechanical and artificial."[131] The particular language one chooses for communication does not change the nature of the language for First Amendment purposes.[132] Furthermore, courts have recognized that "it is frequently the need to convey information to members of the public that dictates the decision to speak in a different tongue."[133] Thus, source code is no different from German or French, which both enjoy First Amendment protection as speech.[134]

Building upon *Reno* allows the conclusion that expression does not lose First Amendment protection just because it interacts with a machine or in this case, a computer. Similarly, "[m]usic . . . is speech protected under the First Amendment . . . [as] [t]he music inscribed in code on the roll of a player piano is no less protected for being wholly functional."[135] Although a computer program is eventually reduced to a form that can be read by a computer, even in "machine-readable" form it can be read and understood only by humans.[136] People can use source code language to express their thoughts on any idea imaginable, and other people can receive and interpret those ideas from the source code. Therefore, the fact that source code language, while

---

129. Yniguez v. Arizonians for Official English, 69 F.3d 920, 934-35 (9th Cir. 1995) (en banc), *vacated on other grounds and remanded sub nom.*, Arizonians for Official English v. Arizona, 520 U.S. 3, *vacated and remanded*, 118 F.3d 667 (9th Cir. 1997).

130. *Yniguez*, 69 F.3d at 934-35.

131. *Id.* at 936 n.21.

132. *See* Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996).

133. *Yniguez*, 69 F.3d at 936.

134. *See id.*

135. *Bernstein*, 922 F. Supp. at 1435 (citing Ward v. Rock Against Racism, 491 U.S. 781, 790 (1989)).

136. Anthony L. Clapes et al., *Silicon Epics and Binary Bards: Determining the Proper Scope of Copyright Protection for Computer Programs*, 34 UCLA L. REV. 1493, 1512 (1987).

both written and read by people, is also capable of instructing a machine should have no effect on First Amendment protection for speech in that particular language.

Policy reasons also exist for declaring source code to be recognized as "pure speech." Often technical speech, like algorithmic source code, is related in the academic context among other scientists, thus deserving constitutional protection. The danger to speech from the chilling of individual thought is especially real in the university setting, where the state acts against a background and tradition of thought and experiment that is at the center of our intellectual and philosophic tradition.[137] Abridging protected freedoms places a straitjacket upon the intellectual leaders in our colleges and universities, imperiling the future of our nation.[138] However, "[o]ur Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers concerned. That freedom is therefore a special concern of the First Amendment . . . ."[139] Thus, people like Bernstein, Karn and Junger must be allowed to develop and express their cryptographic ideas. Their continued breakthroughs in this technology will be critical in the future exchange of information both for this Internet and its next generation.[140] Strong encryption algorithms must continuously be developed, improved, and commercialized to insure reliable protection of electronic communication against potentially disastrous encroachments.[141] For these reasons, electronic source code must be considered speech.

The natural progression of these cases, from *Tinker* up to *Reno*, leads to the conclusion that source code should be recognized as speech. While the *Karn* court decided that source code was more akin to conduct, and the *Junger* court held that source

---

137. Rosenberger v. Rector and Visitors of the Univ. of Va., 515 U.S. 819, 836 (1995).

138. Sweezy v. New Hampshire, 354 U.S. 234, 250 (1957).

139. Keyishian v. Board of Regents of the Univ. of the State of N.Y., 385 U.S. 589, 603 (1967).

140. President's Address Before a Joint Session of Congress on the State of the Union, 34 WEEKLY COMP. PRES. DOC. 129, 139 (Jan. 27, 1998).

141. *See supra* notes 21-28 and accompanying text. The idea is that as computer hackers become increasingly more successful in breaking today's cryptographic codes in commercial applications, developers must strive to stay at least one step ahead of them in offering more and more advanced encryption programs.

code was inherently functional, the *Bernstein* court concluded that source code was speech.[142] The *Bernstein* court reasoned that even when the source code is converted into machine readable object code, the expression of ideas, commands objectives, and other contents does not change.[143] In choosing source code as the "language" to communicate, the decision often may simply be based on a pragmatic desire to convey information to someone so that he or she may understand it.[144] Certainly, this has to be the central kernel which makes source code "pure speech."

B. Standard of Review: Content-Based Versus Content-Neutral

Having established that the publication of cryptographic source code is protected speech does not terminate the inquisition. All restrictions on speech are not per se unconstitutional.[145] Rather, the government's purpose is the controlling consideration in determining whether the licensing provisions of the ITAR and the EAR violate the First Amendment.[146]

Whether certain types of speech have First Amendment protection hinges on whether the restriction is content-based or content-neutral. Content-based restrictions limit communication because of the message conveyed.[147] In *Police Department of the City of Chicago v. Mosley*,[148] the Court struck down a municipality's general prohibition against picketing even though it affected all demonstrators equally.[149] The Court rejected the prohibition because the government does not possess the power to restrict expression of messages, ideas, subject matter, or content.[150] Regulations like these which permit the government to

---

142. *See Junger*, 8 F. Supp. 2d at 716; *Karn*, 925 F. Supp. at 10-11; *Bernstein*, 922 F. Supp. at 1435.

143. *Bernstein*, 922 F. Supp. at 1435.

144. *Id.* (citing Yniguez v. Arizonians for Official English, 69 F.3d 920, 934-35 (9th Cir. 1995)).

145. *See* Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 716 (1931).

146. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

147. Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 47 (1997).

148. 408 U.S. 92, 95 (1972).

149. *Mosley*, 408 U.S. at 100.

150. *Id.*

discriminate on the basis of the content of the message are not to be tolerated under the First Amendment.[151] It is our constitutional right of free expression that is designed to remove governmental restraints from the arena of public discussion and put the decision of what views will be heard into our own hands because no other approach would satisfy individual dignity and choice.[152] Thus, the Court has often found regulations to be content-based regulations on fully protected speech.

Deciding what content is acceptable has caused the Court to determine that some types of speech have a lower First Amendment value and, thus, deserve limited constitutional protection.[153] In *Chaplinsky v. New Hampshire*,[154] the Court observed that "certain well-defined and narrowly limited classes of speech . . . are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."[155] Speech which the Court has historically stated carries a lower First Amendment value includes commercial speech,[156] fighting words,[157] obscenity,[158] and child pornography.[159]

In subjecting some types of speech to a lower level of First Amendment protection, the Court has created a category of speech that has a higher value and that demands a more speech-protective analysis. This higher level of protection extends not only to restrictions on particular viewpoints, but also to prohibitions of public discussion of an entire topic.[160] By def-

---

151. Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd., 502 U.S. 105, 116 (1991) (quoting Regan v. Time, Inc., 468 U.S. 641, 648 (1984)).

152. Cohen v. California, 403 U.S. 15, 22-23 (1971).

153. Geoffrey R. Stone, *Content Regulation and the First Amendment*, 25 WM. & MARY L. REV. 189, 194 (1983).

154. 315 U.S. 568 (1942).

155. *Chaplinsky*, 315 U.S. at 571-72.

156. *See* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 771-72 (1976).

157. *See Chaplinsky*, 315 U.S. at 571-74.

158. *See* Miller v. California, 413 U.S. 15, 23-24 (1973).

159. *See* New York v. Ferber, 458 U.S. 747, 765 (1982).

160. Consolidated Edison Co. v. Public Serv. Comm., 447 U.S. 530, 538 (1980); *see also* Police Dep't of Chicago v. Mosley, 408 U.S. 92, 95 (1972) (holding that a picketing ordinance violated the First Amendment because it created an impermissible distinction between peaceful labor picketing and peaceful picketing).

inition, content-based restrictions distort public debate in a content-differential manner.[161] While a content-neutral ban may disadvantage an entire range of viewpoints, a content-based ban has a greater potential to distort public debate because it disadvantages only a single viewpoint or a particular content.[162] In striking regulations that distort public debate, the Court has established a means of ensuring at least a minimum opportunity for effective expression for those individuals who either lack access to more conventional means of communication or choose a particular means of communication because of its effectiveness.[163]

In *Consolidated Edison Company of New York, Inc. v. Public Service Commission of New York*,[164] the Court found that a public service commission order prohibiting public utility companies from placing inserts discussing controversial issues of public policy in monthly bills was a distortion of the public's access to discussion, debate, and dissemination of information of ideas.[165] The Court held that the commission's order was not a restriction that only regulated the time, place, or manner of speech because the ban only affected certain public controversies; rather, it effectively gave the government control over the choice of permissible subjects for public debate.[166]

Likewise, in *Simon & Schuster v. New York Crime Victims Board*,[167] the Court struck down a law which singled out speech on a particular subject.[168] New York State's "Son of Sam law" required that proceeds from deals made by criminals who sold their stories about their crimes had to be turned over to the state.[169] The state deposited the money in escrow accounts which victims could later claim through civil suits, taking away almost all incentive for criminals to tell their stories. The Court struck down the law for the financial burden that it placed on this particular type of speech and because no reason

161. Stone, *supra* note 153, at 199.
162. *Id.* at 223.
163. *Id.* at 219 n.111.
164. 447 U.S. 530 (1980).
165. *Consolidated Edison*, 447 U.S. at 541.
166. *Id.* at 538.
167. 502 U.S. 105 (1991).
168. *Simon & Schuster*, 502 U.S. at 116.
169. *Id.* at 116-17.

was presented as to why the funds for victim's compensation only came from storytelling proceeds rather than other assets.[170]

Recently, in *R.A.V. v. St. Paul*,[171] a unanimous Court struck down a local bias-motivated criminal ordinance prohibiting the display of symbols which aroused anger, alarm, or resentment in others on the basis of race, color, creed, religion or gender.[172] The Court held that the ordinance was invalid because "it prohibits . . . speech solely on the basis of the subjects the speech addresses."[173] Although the Court recognized that certain forms of speech such as obscenity or defamation can be regulated consistently with the First Amendment because of their constitutionally proscribable content,[174] it also reasoned that majority preferences must be expressed in some fashion other than silencing speech on the basis of its content.[175]

In harmony with the cases above, the ITAR and EAR are content-based because they encompass the entire subject of cryptography and remove it from public discussion. By analogy, if it were illegal to criticize the government's involvement in a war, an entire topic and its accompanying opinions would be removed from public debate. Such a law would mutilate "the thinking process of the community" and is thus incompatible with the central precepts of the First Amendment.[176] Likewise, the ITAR and EAR, because of their inclusiveness, virtually eliminate the entire subject of cryptography from public debate. Any cryptographic data or information with the potential to fall into the hands of a foreign country, or even a foreign national within the United States, must be licensed by the ODTC or the Commerce Department. Thus, virtually all cryptography developers in this country must obtain a license before sharing their discoveries with others because developers cannot control where their own cryptographic programs go after they are released.[177] If

170. *Id.* at 123.
171. 505 U.S. 377 (1992).
172. *R.A.V.*, 505 U.S. at 380.
173. *Id.* at 377.
174. *Id.* at 383.
175. *Id.* at 392.
176. Herbert v. Lando, 441 U.S. 153, 185 n.3 (1978) (Brennan, J., dissenting) (quoting A. MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 27 (1965)).
177. As the Internet is a unique and wholly new medium of worldwide human

developers choose not to obtain a license, they must either remain silent or become subject to criminal and civil sanctions.[178]

Because the ITAR and EAR affect all cryptographic source code, public debate on cryptography is distorted in a content-differential manner. The regulations remove a certain amount of public debate on cryptography from the "marketplace of ideas."[179] Cryptography developers like Bernstein and Karn will be hesitant to share or market their discoveries out of fear of criminal prosecution under the ITAR and EAR. Likewise, the threat of criminal repercussions prevents teachers like Junger from passing knowledge about cryptography across all available mediums of communication.[180] Furthermore, those who decide to approach the edge of the law and disseminate their information to the public via the Internet or other communication methods must edit their cryptographic communications with a fine-toothed comb to remove all material subject to the regulatory provisions. The consequence of these two alternatives is that speech is chilled.

When the government restricts speech in a content-differential manner as it has done with cryptographic source code, such action is justified only upon a showing that the law is both necessary and narrowly tailored to serve a compelling government interest.[181] This standard of review is often called strict scrutiny and is a standard employed by the Court that approaches absolute protection.[182] The government's asserted purpose in the ITAR and EAR is its interest in protecting national security by monitoring and intercepting communications

---

communication which is expected to grow to over 200 million users by 1999, a cryptographic developer would violate the ITAR the moment he posted his algorithm to a web site because the information's accessibility would instantaneously reach to the four corners of the globe. *See generally* Reno v. ACLU, 521 U.S. 844 (1997) (detailing the history and future of the Internet).

178. *See supra* notes 41, 47 and accompanying text.

179. Pilkington, *supra* note 4, at 193.

180. As of the publication date of this Article, Peter Junger had not published any simple encryption programs, known as one-time pads, on his *Computing and the Law* website. Peter Junger, *Computing and the Law* (visited Apr. 19, 1999) <http://samsara.law.cwru.edu/comp_law/index.html>.

181. First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 786 (1978); *see also* R.A.V. v. St. Paul, 505 U.S. 377, 395 (1992) (validating the rule that strict scrutiny review applies to content-based discriminating regulations).

182. Stone, *supra* note 147, at 48.

by foreign intelligence targets and controlling foreign governments' abilities to receive the United States's software products that encrypt data.[183] In support of these premises, courts have held that no governmental interest is more compelling than the security of the Nation.[184] However, that factor alone cannot serve as justification for such a restraint on protected speech.

In *New York Times Co. v. United States*,[185] the Court rejected the government's assertion of national security alone as reason to inhibit free expression and removed a restraining order prohibiting two newspapers from publishing contents of a classified historical study known as the "Pentagon Papers."[186] Even though the case has nine separate written opinions, the majority of the Justices found that a national security interest, without more, was too amorphous a rationale to abrogate the protections of the First Amendment.[187] Furthermore, Justice Black asserted that the security of the nation lay in the very foundation of a constitutional government.[188] The greater the threat to national security, the more imperative the need to preserve the constitutional right of free speech in political discussions so that the government will respond to the will of the people and the changes that may be desired through peaceful means.[189] If the government had the inherent power to halt the free flow of information and ideas based on national security interests alone, it could wipe out the First Amendment and destroy the fundamental liberty of the very people the government hopes to make secure. Thus, the government's sole asserted interest of national security as justification of the ITAR and

---

183. Kerben, *supra* note 3, at 147 (citing Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment at 21, Karn v. United States Dep't of State, 925 F. Supp. 1 (D.C. Cir. 1996)).

184. *Id.*

185. 403 U.S. 713 (1971) (plurality opinion).

186. *See New York Times Co.*, 403 U.S. at 714, 718. Analysis of national security as a compelling governmental interest also arises under this Article's prior restraint analysis below, but even in that context the government likely cannot prevail. *See infra* notes 221-37 and accompanying text.

187. *New York Times Co.*, 403 U.S. at 719.

188. *Id.*

189. *Id.* at 719-20.

EAR is insufficient, without more, to be able to say that a true compelling interest exists.[190]

The government's asserted interest fails to account for the fact that the number of encryption products in foreign countries has steadily risen to the point that foreign corporations are now supplying the American market with encryption products.[191] For this reason, the export control regulations do not *serve* the intended purpose of controlling the growth and availability of encryption products abroad. Rather, the regulations hinder American corporations that want access to the global economy with their encryption products. Thus, these content-based regulations must fail under a strict scrutiny review.

If the ITAR and EAR were deemed not to be content-based regulations as in *Junger*, the Court would analyze them from a content-neutral standpoint.[192] Content-neutral regulations limit expression without regard to the content or communicative impact of the message conveyed.[193] Examples of content-neutral restrictions include zoning ordinances which prohibit operation of adult motion picture theaters within 1,000 feet of residential zones, schools, churches, and parks;[194] laws that limit campaign contributions;[195] and regulations that prohibit demonstrators from sleeping or camping in select national parks.[196]

The Court has applied a broad range of standards to test the constitutionality of content-neutral restrictions. Under a deferential standard, the Court upholds content-neutral laws

---

190. *See* Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1288 (N.D. Cal. 1996). The regulations also use national security in a broad sense by stating that cryptography *"may be used"* to harm national security. 15 C.F.R. § 742.15 (emphasis added). Speech that "may," "could," or "might" prejudice the national security interest in various ways retains absolute protection. *New York Times Co.*, 403 U.S. at 725 (Brennan, J., concurring).

191. Kerben, *supra* note 3, at 148.

192. *See* Junger v. Daley, 8 F. Supp. 2d 708, 720 (N.D. Ohio 1998). The court concluded that the Export Regulations are not content-based because they burden encryption software without reference to any views it may express. *See id.* However, as stated above, this line of reasoning results in the removal of the entire subject of cryptography from public debate. *See supra* note 176 and accompanying text.

193. Stone, *supra* note 147, at 48.

194. *See* City of Renton v. Playtime Theaters, Inc., 475 U.S. 41, 48 (1986).

195. *See* Buckley v. Valeo, 424 U.S. 1, 16 (1976).

196. *See* Clark v. Community for Creative Non-Violence, 468 U.S. 288, 288 (1984).

that rationally further legitimate governmental interests.[197] The Court employs an intermediate standard of review to inquire into the substantiality of the governmental interest and the availability of less restrictive alternatives.[198] Finally, the Court applies a strict standard of review that requires the government's interest be compelling and the challenged restriction be necessary to achieve that interest.[199]

With respect to the ITAR and the EAR, the government claims that source code is not speech at all, but rather, expressive conduct, and as such, a different test, the test utilized in *United States v. O'Brien*,[200] should apply.[201] The Court in *O'Brien* employed a deferential standard.[202] Although the district court in *Bernstein* did not believe that *O'Brien* was the appropriate standard, it nonetheless applied the test and found Bernstein's claims non-frivolous.[203] Even if the regulations were categorized as content-neutral, a higher standard would probably apply rather than the deferential standard used in *O'Brien*. Under *United States v. O'Brien*, the Court promulgated a four-prong test for assessing when a governmental regulation of conduct abridges the First Amendment:

> [A] government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.[204]

Applying these standards to the ITAR and EAR, it is apparent that both regulations fail to satisfy three of the four prongs.

The government admittedly can satisfy the first prong—a regulation of conduct that incidentally restricts speech will be

---

197. *See Renton*, 475 U.S. at 47.
198. Stone, *supra* note 147, at 52.
199. *See* Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982).
200. 391 U.S. 367 (1968).
201. Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996).
202. *O'Brien*, 391 U.S. at 377.
203. *See Bernstein*, 922 F. Supp. at 1437.
204. *O'Brien*, 391 U.S. at 377.

valid if it is "within the constitutional power of the Government."[205] Clearly, the AECA and the ITAR establish that the President may delegate the authority under the law.[206] Likewise, the EAR establishes that the Secretary of Defense has authority under the Export Administration Act.[207]

Although the government can meet the first prong, it is unlikely that it can also meet the second prong of *O'Brien*, which demands that the regulation must further "an important or substantial government interest."[208] As discussed above, the government's interest is in protecting national security by monitoring and intercepting the communications of foreign intelligence targets and controlling foreign governments' abilities to receive United States companies' software products that encrypt data.[209] Recall from above that the regulations failed to *serve* their intended purpose in the context of strict scrutiny review of a content-based regulation.[210] Here, the regulations also fail because they do not actually *further* the same intended purpose but rather handicap American developers of cryptographic software desiring to participate in the global economy. The government naively assumes that controlling the export of encryption software leaving the United States will extinguish its development abroad.[211] In actuality, foreign cryptographic developers are free to enhance their own cryptographic algorithms to levels that potentially are impervious to U.S. code-breaking schemes. As no United States regulation can control proliferation of technology abroad, the regulation cannot be said to further the interest of breaking foreign government's coded communications if foreign governments have acquired strong encryption techniques from foreign sources.[212] Until such time when a global or uni-

---

205. *Id.*

206. 22 U.S.C. § 2778(a)(1) (1994).

207. 50 U.S.C. app. § 2409 (1994).

208. *O'Brien*, 391 U.S. at 377.

209. Kerben, *supra* note 3, at 147 (citing Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment at 21, Karn v. United States Dep't of State, 925 F. Supp. 1 (D.C. Cir. 1996)). The court stated in *Junger* that the government is concerned that foreign intelligence targets can have a debilitating effect on the NSA's ability to collect intelligence. *See* Junger v. Daley, 8 F. Supp. 2d 708, 722 (N.D. Ohio 1998).

210. *Supra* text accompanying notes 189-91.

211. *See Junger*, 8 F. Supp. 2d at 721.

212. As of December 1996, 570 cryptographic products were for sale by foreign

form law exists to control encryption power all over the world, any single American law to that effect will fail to further the government's interest. Therefore, the government fails to satisfy the second prong of the *O'Brien* test.

If the government were to show that the regulations further an important or substantial interest, the third prong would most likely strike a fatal blow against the government. *O'Brien's* third prong requires that "the governmental interest [be] unrelated to the suppression of free expression."[213] As previously discussed, cryptographic source code is speech and has been recognized in court as such.[214] Although the government attempts to win this point by asserting that its interest is only the "functional use" rather than the scientific idea,[215] no legal difference exists between source code written on paper and the same code compiled on a computer disk.[216] Therefore, the government's only rational interest is the suppression of free expression in cryptographic source code that fails the third prong of *O'Brien*.

As the regulations cannot survive the second and third prong, it is also likely that the regulations fail the fourth prong—that "the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest."[217] Although technically the export regulations do not prevent discussions on cryptography, any scientific article published on the Internet would most likely violate the law because of its instant accessibility by foreigners. An Internet publisher of cryptographic software would have to take steps to in-

---

sources in twenty-eight countries, and many possessed encryption power which exceeded the export law limit. Declaration of David Balenson submitted as Exhibit G of Appellee's Opposition to Emergency Motion for Stay, Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (9th Cir. 1997) (No. 97-16686) (visited Apr. 19, 1999) <http://www.eff.org/pub/Legal/Cases/Bernstein_v_DoS/Legal/970917_emerg_stay.opposition>.

213. *O'Brien*, 391 U.S. at 377.

214. Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996); *see supra* text accompanying notes 52-59.

215. *See* Karn v. United States Dep't of State, 925 F. Supp. 1, 11 n.23 (D.D.C. 1996).

216. Kerben, *supra* note 3, at 147; *see also Junger*, 8 F. Supp. 2d at 721 (holding that the export regulations are unrelated to the suppression of free expression because they are not designed to limit the free expression of ideas about the subject of cryptography).

217. *O'Brien*, 391 U.S. at 377.

sure that distribution is confined within the borders of the United States or risk violating the regulations. Such a restriction on such a popular mode of communication ultimately prevents people from sharing ideas on cryptographic subjects.[218] Without the ability to subject one's hypothesis to peer scrutiny, it is unlikely that the hypothesis can be considered factual and worthy of application.[219] Thus, the regulations remove ample alternatives to the study of cryptography.[220] This position is unacceptable because the cryptographic algorithms are protected speech. Because the regulations function to chill this type of speech out of fear of criminal prosecution with no alternatives, the regulations fail the fourth prong of *O'Brien*.

The ITAR and EAR fail to satisfy three of the four *O'Brien* prongs. As a result, these regulations should not be considered as laws controlling expressive conduct, but as laws affecting fully protected speech.

C. Prior Restraint

1. First Amendment Analysis.—Pursuant to the regulations of the ITAR and EAR, Bernstein, Karn and Junger were required to obtain a license before they presented their work at conferences, on Internet web pages and newsgroups, in technical journals, or in any other academically communicative forms. Because they were required to obtain governmental permission before doing these things, the regulations were an unconstitutional prior restraint.

According to the Supreme Court, "it has been generally, if not universally, considered that it is the chief purpose of the [First Amendment] to prevent previous restraints upon publication."[221] The Supreme Court has stated that prior restraints on speech are "the most serious and the least tolerable infringement on First Amendment rights."[222] Thus, "[a]ny prior restraint on expression comes to [the] Court with a 'heavy

218. Kerben, *supra* note 3, at 148.
219. *Id.*
220. *Id.*
221. Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 713 (1931).
222. Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).

presumption' against its constitutional validity."[223]

A statute that makes "the peaceful enjoyment of freedoms which the Constitution guarantees contingent upon the uncontrolled will of an official—as by requiring a permit or license which may be granted or withheld in the discretion of such official—is an unconstitutional censorship or prior restraint upon the enjoyment of those freedoms."[224] However, the government may impose valid time, place, and manner restrictions when they are content-neutral, narrowly tailored to serve a substantial governmental interest, and leave open alternate channels for communication.[225] Even under content-neutral prohibitions, the government may not condition speech on a license obtained from a government official with boundless discretion.[226] To prevent placing unbridled discretion in the hands of governmental officials, standards are required to ensure that licensors do not discriminate against disfavored speech.[227] Without such requirements, the governments and their agencies could virtually eliminate the First Amendment by allowing only speech which is deemed favorable, and disallowing speech that is deemed unfavorable. In such a setting, political commentary, unpopular viewpoints, and even information on cryptography are examples of speech that would either somehow become licensed, or be lost forever.

Again, a governmental rebuttal argument could center upon the notion that the regulations serve a substantial governmental interest—national security. But just as this argument failed under examination in context of the regulations as content-based restrictions, the argument likely fails for the same reasons here.

Recall that in *New York Times Co. v. United States*,[228] the government sought to enjoin newspapers from publishing contents of classified information.[229] In concurrence, Justice Brennan noted that only when the Nation is at war does na-

---

223. *Stuart*, 427 U.S. at 558.

224. Shuttlesworth v. City of Birmingham, 394 U.S. 147, 150 (1969).

225. Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1286 (N.D. Cal. 1996) (citing Clark v. Community for Creative Non-Violence, 468 U.S. 288, 292-93 (1984)).

226. *Bernstein*, 945 F. Supp. at 1286.

227. *See* City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 758 (1988).

228. 403 U.S. 713 (1971). This case is also known as the "Pentagon Papers" case.

229. *New York Times Co.*, 403 U.S. at 714.

tional security warrant an override of the First Amendment.[230] But even then, Justices Stewart and White added that the speech at issue would not "result in direct, immediate, and irreparable damage to our Nation or its people."[231]

In determining the scope of national security, Justice Black realized that the term "security" is broad.[232] Moreover, Justice Brennan stated that the First Amendment tolerates absolutely no prior judicial restraint based upon surmise or conjecture.[233] Thus, speech that "may," "could," or "might" prejudice the national interest in various ways retains absolute protection.[234] In the case of cryptography, there is virtually no difference as the government's concern about cryptography is that it *"may be used* . . . to harm national security."[235] Thus, the government cannot practically eliminate cryptography just because it is a potential risk to national security.

If one assumes that cryptography is a threat to national security, and that fact alone is a substantial governmental interest for which the result is regulated speech, it is probable that the regulations in the ITAR and EAR are not narrowly tailored to further that interest. For the same reasons described above, foreign availability of cryptographic products renders the United States export control scheme virtually ineffective.[236] As stated above, limitations on domestic publication cannot be justified when the same material is available from foreign sources.[237] Thus, it is difficult to imagine that exportation of cryptographic technology originating in the United States would generate a national security threat when equivalent and even superior technology already is available abroad.

2. Due Process Analysis.—Even though the government's national security defense is probably not sufficient to constitute a lawful prior restraint, narrowly drawn standards exist to con-

230. *Id.* at 726 (Brennan, J., concurring).
231. *Id.* at 730 (Stewart & White, JJ., concurring).
232. *Id.* at 719.
233. *Id.* at 725 (Brennan, J., concurring).
234. *New York Times Co.*, 403 U.S. at 725 (Brennan, J., concurring).
235. 15 C.F.R. § 742.15 (1998) (emphasis added).
236. *See supra* notes 185-91 and accompanying text.
237. *See* ACLU v. Reno, 929 F. Supp. 824, 882 (E.D. Pa. 1996).

trol the licensing scheme procedurally. The government may enact a licensing scheme, but must establish clear procedures with little discretion to the licensing authority and must be careful not to present peculiar dangers to constitutionally protected speech.[238] To avoid placing "unbridled discretion in the hands of a government official or agency," the licensing scheme must contain adequate safeguards.[239]

The Court has, in *Freedman v. Maryland*,[240] set forth procedural safeguards to evaluate licensing schemes. First, any restraint prior to judicial review can be imposed only for a specified brief period during which the status quo must be maintained.[241] The underlying policy for this requirement is that if a license is not issued in a reasonable period of time, undue delay may result in unconstitutional suppression of protected speech.[242]

Here, under the ITAR, the decision of the ODTC is not limited by any amount of time.[243] The EAR does require that an application for an export license be resolved or referred to the President within ninety days of registration of the application.[244] However, the EAR is silent on any time limitations on applications referred to the President, so the ninety-day time limits become meaningless as it would be possible for the President to indefinitely retain the license application once it reaches that level. Therefore, both the ITAR and the EAR fail to require a decision within a specified brief period of time.

The second *Freedman* procedural safeguard requires expeditious judicial review of the licensing decision.[245] The ITAR provides for no judicial review of licensing decisions, and the AECA

---

238. *See* Freedman v. Maryland, 380 U.S. 51, 56 (1965).

239. *See* City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 757-58 (1988).

240. 380 U.S. 51, 58 (1965).

241. *Freedman*, 380 U.S. at 58-60; *see also* FW/PBS, Inc. v. City of Dallas, 493 U.S. 215, 227 (1990) (discussing *Freedman*).

242. *Freedman*, 380 U.S. at 57.

243. Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1289 (N.D. Cal. 1996) (citing 22 U.S.C.A. § 2278(h) (West 1997)).

244. 15 C.F.R. § 750.4(a)(1) (1998).

245. *Freedman*, 380 U.S. at 58-60; *see also FW/PBS*, 493 U.S. at 226 (holding that "[t]he core policy underlying *Freedman* is that the license for a First Amendment-protected business must be issued within a reasonable period of time").

establishes that items designated as defense articles are unreviewable.[246] The only appeal available under the EAR is through the Export Administration that administered the initial decision, and decisions made on that appeal are final and unreviewable.[247] This scheme can hardly be said to satisfy the requirement of prompt judicial review in the event that a license is denied in error.

The final *Freedman* safeguard specifies that the censor must bear the burden of going to court to suppress speech and once there, bear the burden of proof.[248] As no recourse exists under either the ITAR or the EAR for someone denied a license, no burden exists for either the ODTC or the Export Administration to go to court to justify denial.[249] *Freedman* refuses to require that the party desiring to be licensed bear the burden of bringing judicial action; however, the ITAR and EAR do not provide that the government carry such a burden. Thus, the regulations completely fail to account for this procedural safeguard.

Therefore, the controls placed on cryptography ignore the procedural safeguards mandated by the Supreme Court for regulatory licensing schemes. Consequently, the ITAR and EAR are an unconstitutional prior restraint in violation of the First and Fifth Amendments.

D. The Fourth Amendment

The most significant application for cryptography rests in its ability to ensure private communication. Privacy has long been a cherished principle which has found protection in the First and Fourth Amendments.[250] The government's control of cryptography, resulting in its ability to freely monitor electronic communications, raises issues pertaining to unreasonable searches and seizures. However, the Fourth Amendment grants people the

---

246. *Bernstein*, 945 F. Supp. at 1289.

247. 15 C.F.R. § 756.2(c) (1998).

248. *Freedman*, 380 U.S. at 58-60; *see also FW/PBS*, 493 U.S. at 227 (holding that the censor must bear the burden of going to court to suppress the speech and must bear the burden of proof once in court).

249. *See Bernstein*, 945 F. Supp. at 1289.

250. *See* Henry R. King, *Big Brother, the Holding Company: A Review of Key-Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224, 249 (1995).

right to privacy while at the same time granting the government the ability to conduct investigations in a reasonable manner for the purposes of law enforcement.[251] As stated earlier, detracting from the government's ability to engage in effective law enforcement runs the risk of endangering national security, but to alleviate that risk, it hardly seems necessary to enact laws that retard the growth of cryptography in this country, while allowing it to flourish abroad.

The right to privacy was initially stated in terms of the right to be left alone, which was first articulated by Justice Brandeis in his dissent in *Olmstead v. United States*.[252] There, federal agents installed wiretaps in the basement of a suspected bootlegger's building and obtained a conviction with evidence obtained from the wiretaps.[253] Although the majority stated that a party's Fourth Amendment rights could not be infringed because the wiretapping did not constitute a search and seizure under the meaning of the Fourth Amendment,[254] Justice Brandeis feared that if the government were allowed to become a law-breaker, it would invite every person to become a law unto himself to the point of anarchy.[255] He believed the evil incident of invasion of privacy through electronic communication to be far greater than that involved in tampering with the mails, which enjoyed protection by constitutional amendments.[256] To protect the right to privacy, Justice Brandeis asserted that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[257] Any use of facts gained by such an intrusion as evidence in a criminal proceeding would violate the Fifth Amendment.[258]

---

251. Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 191 (1996).

252. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

253. *Olmstead*, 277 U.S. at 457.

254. *Id.* at 466.

255. *See id.* at 466, 485 (Brandeis, J., dissenting).

256. *Id.* at 475. Justice Brandeis actually was referring to the telephone, which itself is a form of electronic communication. *See Ex parte* Jackson, 96 U.S. 727 (1877) (arguing that no difference exists between a sealed mailed letter and a private telephone message).

257. *Olmstead*, 277 U.S. at 478.

258. *Id.* at 479.

The Court adopted Justice Brandeis's words later in *Katz v. United States*.[259] Here, federal agents attached an electronic listening and recording device to the outside of a public phone booth in the belief that Katz used the booth to transmit wagering information by telephone.[260] Based on the evidence obtained with the eavesdropping device, Katz was convicted. The Court held that Katz was entitled to Fourth Amendment protection for his conversations and that a physical intrusion into the area he occupied was not necessary to invoke the Amendment's protections.[261] Rather, "the Fourth Amendment protects people, not places."[262] Justice Harlan introduced the idea of a "reasonable" expectation of privacy in his concurring opinion, and set forth a twofold rule.[263] First, a person must have exhibited an actual (subjective) expectation of privacy, and second the expectation must be one that society is prepared to recognize as "reasonable."[264] The Court realized that people expect that their conversations will be private, and opportunities of even temporary privacy among participants in expectation of freedom from intrusion are recognized as reasonable.[265]

With cryptography, the expectation of privacy is the same as that advanced in *Katz*. Courts have held that when a person takes affirmative steps, an expectation of privacy is created that is equal to the protection that exists in one's home.[266] Likewise, cryptographic algorithms enable users to prevent unauthorized intrusion in a similar manner to a sealed envelope or a locked door. Because cryptographic technology works to ensure that only the sender and receiver understand the encrypted communication, a sense of privacy is the intended and achieved result. As cryptographic transmissions are relatively new in the private sector, one can easily assume that the vast majority of

---

259. 389 U.S. 347 (1967).
260. *Katz*, 389 U.S. at 348.
261. *See id.* at 348-59.
262. *Id.* at 351.
263. *Id.* at 361. (Harlan, J., concurring).
264. *Id.*
265. *Katz*, 389 U.S. at 361.
266. King, *supra* note 250, at 250; *see also* United States v. Chadwick, 433 U.S. 1 (1977) (holding that by placing items in a locked footlocker, respondents manifested an expectation that the contents would remain free from public examination in the same sense that one locks the doors of his home against intruders).

electronic transmissions on any given day are not encrypted. Those users who make the extra effort to encrypt their transmissions almost certainly do so with the idea of ensuring that others cannot intercept and read the content of the messages. Thus, a person encrypting messages certainly exhibits an actual expectation of privacy, especially when he or she selectively encrypts some messages and does not encrypt others. Moreover, it certainly seems no more reasonable to place a letter in an envelope, place a lock on a personal locker, or draw the blind at the voting booth than it does to take steps to ensure electronic message security.

As presently drafted, the ITAR and the EAR both fail to recognize that cryptographic source code enables people to preserve a reasonable expectation of privacy in cyberspace. Because the ITAR and EAR effectively hinder the development of cryptographic technology, only cryptographic algorithms that were available before the regulations were enacted or others which have become licensed by the ODTC or Commerce Department can be utilized by the public. Thus, the government has effectively reduced the technology to the lowest common denominator,[267] and practically removed incentive to tread any further. Moreover, merely because the government may or may not be capable of breaking a given cryptographic communication does not tarnish the sender's and recipient's expectation of privacy. The government surely owns letter openers that are capable of opening people's mail, and it also possesses the technology to electronically eavesdrop on telephone communications; however, in each instance, the government must usually obtain a warrant before infringing the target's privacy.[268] Likewise, the ITAR and EAR should not be used as tools to enable the government to break anyone's cryptographic code upon a whim. However, by controlling the development of the technology, the government has maintained the capability to invade a person's privacy without the trouble of obtaining a warrant.

---

267. *See* Reno v. ACLU, 521 U.S. 844, 852-58 (1997).
268. *See* Berger v. New York, 388 U.S. 41, 49 (1967).

V. ALTERNATE PROPOSAL

As the ITAR and EAR are inadequate to serve the national security interests put forth by the government, alternate proposals must be applied to strike a more precise balance to the government's interests and those of developers like Bernstein, Karn, and Junger. Because technology constantly changes, any proposal that may work today may be wholly unworkable tomorrow. However, prudent steps are steps in the right direction.

First, Congress can take the initiative in revamping the laws from which the ITAR and EAR derive their power. Software industry representatives have publicly urged Congress to pass a resolution making such reforms.[269] Although amending the current laws may patch known gaps, entirely new legislation that is fully compatible with the unique characteristics of the Internet is necessary.

Congress is currently considering a bill proposing amendments to the *United States Code*, entitled Security and Freedom Through Encryption (SAFE) Act, which would affirm the rights of Americans to use and sell encryption and would relax export controls on encryption.[270] SAFE affirms the freedom to use the strongest possible encryption and allows the United States to compete in the rapidly growing market for strong encryption products.[271]

This bill does not seek to control cryptography by any type of licensing process to preserve governmental interests, but rather establishes the National Electronic Technologies (NET) Center within the Department of Justice to serve law enforcement in obtaining access to encrypted electronic communications.[272] NET will not only develop efficient methods and improve the efficiency of existing methods of accessing such plaintext, but will also investigate techniques and technologies to facilitate access to communications and electronic informa-

---

269. Pilkington, *supra* note 4, at 208.

270. H.R. 850, 106th Cong. (1999).

271. Americans for Computer Privacy, *Bills in Congress* (visited Apr. 19, 1999) <http://www.computerprivacy.org/bills/>.

272. Thomas Legislative Information on the Internet, *Bill Summary & Status for the 106th Congress-H.R. 850* (visited Apr. 19, 1999) <http://thomas.loc.gov/cgi-bin/bdquery/z?d105:HR00695:@@@L>.

tion.[273] The bill prohibits any person in lawful possession of a key to encrypted communications from being required by federal or state law to relinquish to another person control of that key, with an exception for law enforcement purposes.[274] Finally, the bill requires the President to negotiate with other countries to establish international agencies to preserve national security, safeguard privacy, and prevent commercial espionage.[275]

If this bill becomes law, the First Amendment issues discussed above become moot. Development and dissemination of cryptographic algorithms would no longer be controlled; thus, speech in the form of cryptographic source code would not be chilled. SAFE does not present prior restraint concerns because the bill does not include any licensing process. Even with the SAFE bill, privacy considerations remain. However, established law on appropriate searches and seizures would offer protection. Thus, if SAFE can pass both Houses of Congress and obtain the President's signature, an excellent alternative to both the ITAR and EAR can become the law of the land.

If Congress is not able to enact SAFE or some other solution, courts will see more attacks on the ITAR and EAR in an effort to ensure that export controls on encryption are held to First Amendment strict scrutiny standards. As *Bernstein*, *Karn*, and *Junger* have yielded completely opposite results on the same legal questions, it is likely that the Supreme Court controls the future of the growth and prosperity in cryptography.

VI. CONCLUSION

As *Bernstein*, *Karn*, and *Junger* collectively prove, the courts are not settled on the proper level of protection to apply to cryptography. Only if these export control laws are found by the courts to be unconstitutional suppressions and prior restraints on pure speech can the First Amendment and our right to privacy survive unscathed. Anything less will surely change the fu-

273. *Id.*
274. *Id.*
275. *Id.*

ture course of electronic communication. Extending full First Amendment protection to cryptography will serve as a springboard for commerce and communication into the millennium.

Norman Andrew Crain