University of Arkansas at Little Rock Law Review

Volume 21 | Issue 2 Article 4

1999

Building Castles Made of Glass—Security on the Internet

Joe Baladi

BUILDING CASTLES MADE OF GLASS—SECURITY ON THE INTERNET

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

Benjamin Franklin

I. INTRODUCTION

As the internet, with over 60 million users,[1] displaces traditional forms of communication, constitutional issues implicating the First, Fourth, and Fifth Amendments will need to be resolved. Recent polls demonstrate that the increase in the number of computers has heightened the public's concern about privacy issues.[2] Ironically, many ardent law enforcement supporters have lamented that the government is watching as never before.[3] Computers, more specifically the internet, need not infringe the privacy protections Americans hold so dear. While unfettered access to computer records would indeed stifle privacy, recent technological advances have made it possible to ensure private communication over the internet.

Encryption allows internet users to send and receive information in code, decipherable only by a person with the appropriate "key."[4] Legislators have proposed bans on certain types of encryption programs, and some proposals mandate unrestricted access to the keys. These proposals would force users of encryption to leave their keys to private files with law enforcement officials. In effect, people communicating on the internet would live in a glass house. For very apparent reasons, those who oppose such proposals cite the liberty and privacy interests protected by the First, Fourth, and Fifth Amendments. Additionally, the United States District Courts for the Northern District of California and the Northern District of Ohio have recently decided cases regarding the use and export of encryption technology.[5] This comment seeks to discuss these conflicting decisions, the recent proposals to regulate encryption, and the resulting Constitutional implications.

---

1. *See* Lawrence Freedman, *Computers, Viruses and War,* NEWSWEEK, Apr. 27, 1998, at 4 (estimating that up to 70 million people worldwide use the internet).

2. In a Harris Poll published March 16, 1998, in BUSINESS WEEK, 80% of respondents stated they were very or somewhat concerned that credit card data would be stolen if used online. *See Online Insecurity,* BUSINESS WEEK, Mar. 16, 1998, at 102.

3. *See* Simon Lazarus, *Talking in Code,* THE RECORDER, Apr. 1, 1998, at 6.

4. A "key" is a digital formula used to convert ciphertext into plaintext. *See* Samuel Lewis, *Difficult no more: Encryption sheds its "Bad" Reputation; Point-and-click Security On-Line,* 218 N.Y.L.J. S4 (1997). A key is unique to the recipient and, therefore, communications can only be read by the proper recipient. *See id.*

5. *See* Junger v. Daley, U.S. Secretary of Commerce, 8 F. Supp. 2d 708 (N.D. Ohio 1998); *See* Bernstein v. United States Dep't of State, 974 F. Supp. 1288 (N.D. Cal. 1997).

Sections II and III consist of a brief historical background of the internet, and a description of the regulatory framework at issue in the conflicting decisions. Sections IV and V discuss the conflicting cases and recent congressional proposals, respectively. Finally, the constitutional implications are explored in light of the conflicting decisions and congressional proposals.

II. HISTORICAL BACKGROUND

A. The Internet

In the early 1960s, the Cold War was in full swing, citizens were installing bomb shelters, and children were taking cover under their desks in preparation for a nuclear attack. The military decided the United States needed a communication network that would work even if large portions of the support network were destroyed or lost.[6] The internet was designed under contract from the Advanced Research Projects Agency (ARPA).[7] ARPA connected four universities via computer: UCLA, Stanford, the University of California Santa Barbara, and the University of Utah.[8]

Initially, only researchers, mathematicians, engineers, and computer experts used the internet.[9] In the early 1970s, personal home computers were not yet available, and the internet system was very complex, even for experts. The internet began to come of age in the 1970s with the development of Interface Message Processors.[10] Subsequently, Bob Kahn at ARPA and Vint Cerf at Stanford developed Transmission Control Protocol (TCP),[11] which allowed remote, diverse computers to communicate with each other.[12]

Gradually, commands for e-mail and file transfer protocol became easier to understand and utilize for people other than physicists, engineers, mathematicians, and computer experts.[13] Eventually more and more people used the internet, and university libraries updated to electronic catalogues offering their

---

6. *See* Barry M. Leiner et al., *Internet Society (ISOC) All About the Internet: A Brief History of the Internet* (visited July 29, 1998) <http://www.isoc.org/internet-history/brief.html>.

7. *See* Walt Howe, *Delphi FAQs: A Brief History of the Internet* (visited July 3, 1998) <http://www.delphi.com/navnet/faq/history.html>.

8. *See id.*

9. *See id.*

10. *See id.*

11. *See* Leiner, *supra* note 6. *See also* Vint Cerf, *A Brief History of the Internet and Related Networks* (visited August 29, 1998) <http://www.simmons.edu/~pomerant-/techcomp/cerf.html>. The term "internet" is attributed to Vint Cerf and Bob Kahn. *See* Dave Kristula, *The History of the Internet* (visited 7/29/98) <http://www.davesite.com/webstation/net-history.shtml>.

12. *See* Leiner, *supra* note 6. *See also* Cerf, *supra* note 11.

13. *See* Leiner, *supra* note 6. *See also* Cerf, *supra* note 11.

resources to the world. The number of sites at this time remained small, yet more and more organizations and universities were connecting to the internet.[14]

The World Wide Web was a new protocol developed in the early 1990's by Tim Berners-Lee and Al Vezza.[15] A graphical browser, Mosaic, developed by Marc Andreesen simplified the World Wide Web and propelled it to its current prominence.[16] Initially, users could not route internet communication across the country without going through the government-funded network. However, in the early 1990s, independent commercial networks increased and made it possible to bypass the government network.[17] In May of 1995, all internet traffic traveled through independent commercial networks.[18] Currently, the internet has over 50,000 networks on all continents, with over 30,000 in the United States.[19]

B. Encryption

Encryption has been used in many forms throughout history. Almost everyone from military generals to children has sent coded messages in an attempt to secure privacy. Many people believe the allied forces were able to shorten World War II because of their ability to break Japanese and German codes.[20] The export of encryption technology was forbidden after the war, and encryption was classified as a munition.[21] Domestic use was still allowed because of the very limited practical domestic application.[22] The internet has now created tremendous demand and abundant uses for encryption technology. For the internet to realize its full potential, businesses and private individuals will demand confidential communications. Individuals need to protect credit card numbers, bank account numbers, and various other confidential information. Corporations will need to communicate business plans, transfer currency, review financial statements, and debate operational guidelines to remote business units around the globe. Encryption technology allows for this

---

14. *See* Walt Howe, *Delphi FAQs: A Brief History of the Internet* (last updated July 3, 1998) <http://www.delphi.com/navnet/faq/history.html>.

15. *See id.*

16. *See id.* Andreesen is also the brains behind Netscape, one of the most successful graphical browsers to date. *See id.*

17. *See id.* Initially, the government funded the supporting structure for the internet. *See id.*

18. *See* Walt Howe, *Delphi FAQs: A Brief History of the Internet* (updated July 3, 1998) <http://www.delphi.com/navnet/faq/history.html>. AOL, Prodigy, and Compuserve came online and now account for the overwhelming majority of internet service providers. *See id.*

19. *See* Leiner, *supra* note 6.

20. *See* Lazarus, *supra* note 3, at 6.

21. *See* Lazarus, *supra* note 3, at 6. *See also infra* Section III.

22. *See* Lazarus, *supra* note 3, at 6.

communication or transaction while preventing the unauthorized interception, viewing, copying, altering, or forging of transmissions.[23]

Encryption involves the use of algorithms, which instruct a computer to encrypt plaintext into a coded, unintelligible message called ciphertext.[24] Once converted to ciphertext, the plaintext can only be decrypted to plaintext with the correct "key" held by the intended recipient.[25] The two types of encryption are symmetric and asymmetric.

Symmetric encryption involves use of the same key to encrypt and decrypt. The disadvantage to symmetric encryption is that the decryption key has to be disclosed to more than the intended recipient because the same key is used by the sender and the recipient, which makes it more likely that the key will fall into a third party's hands.[26] Asymmetric encryption heightens security because the public encryption key is made available to anyone, while only the recipient holds the private decryption key.[27] Through this method, anyone can use the public key to encrypt a message to the holder of the private key.[28]

The software for encryption is available in object code and source code.[29] Object code is written in binary code.[30] Source code is written in complicated computer programming language such as Fortran.[31] The two codes are, in essence, instructions for a computer to perform some task.[32] They are also interchangeable; however, a computer cannot execute source code commands without interpreter software.[33]

The technological advances in personal computers that can encrypt and decrypt messages create a problem for the FBI because they may not be able to crack the code to monitor illegal activity.[34] Encryption code is measured in bits and increases exponentially in strength with each added bit.[35] Encryption

---

23. *See Junger*, 8 F. Supp. 2d at 712.

24. *See id.* Plaintext is a document or message as written by a human. Ciphertext is the process of transforming plaintext to an unintelligible message. *See id.*

25. *See* Lewis, *supra* note 4, at 54. *See also* Lazarus, *supra* note 3, at 6.

26. *See* Lewis, *supra* note 4, at 54.

27. *See* Lewis, *supra* note 4, at 54. The keys correspond mathematically so that the communication encrypted by the public key can only be decrypted by the related private key. *See* Lewis, *supra* note 4, at 54. Anyone wishing to communicate with the holder of the private key uses the public key for that person to encrypt the message. *See* Lewis, *supra* note 4, at 54.

28. *See* Lewis, *supra* note 4, at 54.

29. *See Junger*, 8 F. Supp. 2d at 712.

30. *See id.* (binary code consists of computer instructions written as 1's and 0's).

31. *See id.* at 712 & n.3.

32. *See Junger*, 8 F. Supp. 2d at 712.

33. *See id.* Source code is understandable by one proficient in technical computer programs, and a computer may understand the source code with software that will interpret source code to object code for the computer. *See id.* at 712 & n.3.

34. *See* Lazarus, *supra* note 3, at 6.

35. While 40-bit encryption may take hours to break, 128-bit encryption would take a

of fifty-six bit length or less can be cracked[36] and exported legally. Any encryption of greater bit length cannot be exported without a waiver from the Executive Branch. The Department of Commerce and the FBI are concerned that the proliferation of encryption will make it more difficult to monitor and apprehend terrorists, which will threaten the security of the United States.

III. ENCRYPTION REGULATION

A. Prior Regulatory Framework

The regulations on encryption initially were the International Traffic in Arms Regulations ("regulations"),[37] which are the implementing regulations for the Arms Export Control Act ("Act").[38] The regulations give the President authority to control "the import and export of defense articles . . . and to provide foreign policy guidance to persons . . . involved in the export and import of such articles."[39] Any item the President designates as a defense article is a part of the United States Munitions List ("USML").[40] In order for someone to import or export an item on the USML, an export license must be procured.[41]

The Secretary of State, under authority from an executive order, promulgated the regulations.[42] Section 121.1 lists categories of items covered by the USML, and includes "cryptographic (including key management) systems, . . . components or software with the capability of maintaining secrecy

---

trillion years to break with current technology according to Netscape's chief scientist. *See* Richard R. Mainland, *Congress Holds the Key to Encryption Regulation*, NAT'L. L.J., Apr. 20, 1998, at B16 n.1.

36. If a key is sufficiently short, one intercepting ciphertext can break the code by a brute force search. This entails attempting every key combination until the plaintext message is obtained. *See* COMMITTEE TO STUDY NATIONAL CRYPTOGRAPHY POLICY, NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 63 (1996). One can crack encryption software of this length easily, and stronger encryption is readily from foreign producers. *See E-Commerce & Y2K: What's Ahead For Small Business: Hearing Before the United States Senate Committee on Small Business*, 105th Cong. (1998) (statement of Harris N. Miller, President, Information Technology Association of America). The result will be that high-tech firms in the United States stand to lose up to $65 billion and numerous jobs. *See id.*

37. 22 C.F.R. §§ 120-30 (1994).

38. 22 U.S.C. § 2778(b) (1996).

39. *See id.*

40. *See id.*

41. *See id.* The Director of the United States Arms Control and Disarmament Agency decides which items are licensed. *See* 22 U.S.C. § 2778(a) (1994).

42. *See* Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1283 (N.D. Cal. 1996).

or confidentiality of information . . . ."[43] Encryption technology, therefore, needs a license for import or export because it is listed on the USML. The regulations do allow for a "commodity jurisdiction procedure" if doubt exists as to whether an item is covered by the USML.[44]

B. Current Regulatory Framework

The current regulatory framework is slightly different due to Executive Order 13,026, entitled "Administration of Export Controls on Encryption Products."[45] In November of 1996, President Clinton transferred jurisdiction of nonmilitary encryption products to the Commerce Department under authority of the Export Administration Act of 1979[46] and the Export Administration Regulations.[47] Encryption items designated as defense articles under the USML are now listed on the Commerce Control List.[48] However, the White House later clarified the Executive Order by stating that the USML would continue to list encryption items designed for military application.[49] The Executive Order contains an admonition that the "export of encryption . . . must be controlled because of such software's functional capacity, rather than because of any possible informational value . . . ."[50] These export regulations are in effect to this day.[51]

The Bureau of Export Administration ("Bureau"), a division of the Commerce Department, amended the Export Administration Regulations "by exercising jurisdiction over, and imposing new combined national security and foreign policy controls on, certain encryption items that were on the [USML]."[52] The amended regulations contain a category called "Encryption Items" defined as "all encryption commodities, software, and technology that contain encryption features and are subject to the [Export Administration

43. 22 C.F.R. § 121.1 XIII(b)(1) (1993).

44. *See* Bernstein v. United States Dep't of State, 974 F. Supp. 1288, 1293 (N.D. Cal. 1997).

45. Exec. Order No. 13,026, 15 C.F.R. 730-74 (1996).

46. 50 U.S.C. app. § 2401 (1991).

47. *Id. See also* 15 C.F.R. § 730 (1997).

48. *See Bernstein*, 974 F. Supp. at 1293.

49. Encryption items "specifically designed, developed, configured, adapted, or modified for military applications (including command, control and intelligence applications)" remain on the Regulations and under the jurisdiction of the State Department. *See* 61 Fed. Reg. 68,633 (1996).

50. *See supra* note 45.

51. The EAA lapsed in 1994, but the President, under authority of the International Emergency Economic Powers Act, extended the regulations, and has done so each year since. *See Junger*, 8 F. Supp. 2d at 713.

52. 15 C.F.R. §§ 730-74 (1996).

Regulations]."[53] Generally, the Bureau must grant a license to export any Commerce Control List item, though there are a few exceptions.[54]

The Bureau regulations designate three categories of encryption items. ECCN 5A002 lists encryption commodities, ECCN 5D002 lists encryption software, and ECCN 5E002 lists encryption technology.[55] The regulations define the export of controlled encryption object[56] and source code[57] software as "downloading, or causing the downloading of, such software to locations . . . outside the U.S. . . . ."[58] Thus, someone posting encryption software on the internet is exporting it.[59] Finally, technical assistance regulations were added. Technical assistance in the development of encryption items to a foreigner requires a license if the encryption items are controlled domestically under ECCN 5A002 and 5D002.[60] However, the regulation states "that the mere teaching or discussion of information about cryptography . . . by itself would not establish the intent described in this section, even where foreign persons are present."[61]

In order to export an item on the Commerce Control List, one must request an ECCN classification from the Bureau.[62] An export license is required for all countries except Canada if an item falls under one of the ECCN classifications.[63] Another exception to the licensing requirement states that a license for export is not required for encryption source code in printed form, such as a textbook or journal.[64] Exceptions also exist for commercial encryption items, which include mass-market encryption software, key-recovery software, and non-recovery encryption items up to fifty-six bit key

---

53. 15 C.F.R. § 772 (1996).

54. *See* 15 C.F.R. §§ 740-44 (1996).

55. *See* 15 C.F.R. § 774 (Supp. I 1996). The definition of Encryption software (ECCN 5D002) is "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software." 15 C.F.R. § 772.

56. Object code is defined as "[a]n equipment executable form of a convenient expression of one or more processes ("source code" (or source language)) that has been converted by a programming system." 15 C.F.R. § 772.

57. Source code is defined as "[a] convenient expression of one or more processes that may be turned by a programming system into equipment executable form." *See id.*

58. 15 C.F.R. § 734.2(b)(9)(B)(ii) (1996).

59. *See id.* There is an escape clause of sorts because it is not an export over the internet if the ". . . person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States." *Id.* However, anyone with knowledge of the internet knows that it would be virtually impossible for anyone to verify the destination of software being downloaded from a remote site.

60. *See* 15 C.F.R. § 736.2(b)(7)(ii) (1996).

61. 15 C.F.R. § 744.9(a) (1996).

62. *See* 15 C.F.R. §§ 740-44 (1996).

63. *See* 15 C.F.R. § 742.15(a) (1996).

64. *See* 15 C.F.R. § 734.3(b)(2) (1997).

length if there is a commitment to develop recoverable items.[65] Generally, the exceptions listed relate to items currently available to the public. Consequently, the exceptions would not apply to encryption commodities not specifically listed and already available to the public.

Currently, any citizen or corporation may use any form or strength of encryption domestically, and the technology may be distributed domestically.[66] A person exporting the technology without a license faces significant criminal penalties.[67] As of January 1997, the limit on key length for export is fifty-six bits, but only if the company commits to development of a key recovery system.[68] Anyone not committing to a key recovery system cannot export the encryption products without incurring criminal punishment including imprisonment.[69] Against this backdrop, two significant cases have emerged which will have a dramatic impact on the future course of encryption regulations.

IV. CONFLICTING DECISIONS

We are at a fork in the road regarding the future of communication, commerce, and privacy on the internet. Each path leads to opposite ends of the same destination. The destination is a time when medical records are stored and transmitted from physician to physician over internet connections, a time when banking, paying bills, negotiating contracts, sending electronic mail, and many other everyday activities are conducted via internet connections. One path leads us to a secure environment in which encryption technology plays a role in protecting the liberty and privacy interests firmly established in the Constitution. The other path leads to a future that enables law enforcement officials, hackers, and others to monitor medical records, banking information, energy consumption via electronic billing, and purchasing habits among the many other factors of everyday life. To date, Congress has not indicated that it has the desire to deal with the issue of encryption technology. The courts,

---

65. *See* 15 C.F.R. § 742.15(b)(3) (1996). The regulations, in the author's opinion, contain what amounts to extortion in not allowing the export of encryption, unless there is a commitment to develop key recovery.

66. *See* 22 C.F.R. § 123 (1996).

67. *See* 22 U.S.C. § 2778(c) (1996). The violation of the Act carries maximum penalties of $1,000,000 or up to 10 years in prison, or both. A violation of the EAA is subject to a $50,000 fine or five times the value of the exports, whichever is greater, or imprisonment up to five years, or both. *See* 50 U.S.C. § 2410(a) (1994).

68. Key recovery entails "depositing", or "escrowing", the key with a third party so that law enforcement officials may have ready access after following standard criminal investigation procedures. *See* Rick Henderson, *Clipping Encryption; Data Encryption Control*, REASON, May 1998, at 7.

69. *See supra* note 45.

therefore, have the role of preserving the liberty and privacy interests of internet communication, while considering the government's legitimate concern for monitoring criminal activity.

A. The *Bernstein* Decision

Daniel J. Bernstein developed an encryption algorithm named "Snuffle."[70] Bernstein made Snuffle public in two ways: in an academic paper and in a high-level computer language.[71] Both communications revealed the methods for encryption and decryption.[72] Bernstein requested a classification by the State Department to determine whether Snuffle, as revealed in source code and the academic paper, was controlled by the regulations.[73] The State Department classified Snuffle as a defense article that should be listed on the USML and subject to licensing prior to export.[74] Concerned that he would not be able to teach, discuss, or publish Snuffle with other academicians, Bernstein challenged the Act and the regulations on the theory that they violate the First Amendment.

The United States District Court for the Northern District of California held in *Bernstein I*, that "source code is speech for purposes of the first amendment" and that the case presented a colorable constitutional claim.[75] *Bernstein II* presented the court with the question of whether export-licensing regulations on encryption violate the First Amendment.[76] The Court concluded that the licensing system acts "as an unconstitutional prior restraint in violation of the First Amendment" because it fails to "provide for a time limit on the licensing decision, for prompt judicial review, and for a duty on the part of the [State Department] to go to court and defend a denial of a license . . . ."[77] *Bernstein III* presented the question of whether the licensing requirements for the export of encryption technology constitute an unconstitutional infringement

---

70. *See Bernstein*, 974 F. Supp. at 1293 (describing snuffle as a private-key encryption system).

71. *See id.*

72. *See id.* Recall that source code is not readable by a computer without interpreter software, but once interpreted to a binary system of 0's and 1's, the computer can encrypt and decrypt. *See Junger*, 8 F. Supp. 2d 708.

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

74. *See id.* at 713.

75. *See* Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1438 (N.D. Cal. 1996). The *Bernstein I* court was the first ever to hold that source code is speech protected by the First Amendment. *See id.*

76. *See Bernstein*, 945 F. Supp. at 1285.

77. *Id.* at 1290. It should be noted that the holding in the instant case consists of correctable defects. The court did not go so far as to say the government could not, under different circumstances, regulate encryption technology. *Id.*

on speech.[78] The defendants argued that a facial challenge to the regulations did not apply because the encryption software is conduct, not expression.[79] The Court did not agree with the defendant's speech/conduct distinction noting that "while the export of a commercial cryptographic software program may not be undertaken for expressive reasons, that same activity . . . is often undertaken by scientists for purely expressive reasons."[80] The nature of a scientist, academician, and scholar is to teach, publish, and lecture—activities the government aims to regulate.[81]

The *Bernstein I* decision noted that the academic paper on Snuffle constituted speech of the most protected kind.[82] The defendants, citing *Texas v. Johnson*,[83] argued that there must be a sufficient nexus between the conduct and expression to constitute First Amendment protection.[84] The claim is that encryption is functional software not intended to convey any message.

The court could find no difference between computer language and a foreign language.[85] Indeed it is difficult to understand a distinction. There are mathematicians, computer experts, physicists, and other academicians who readily understand source code. The distinction is that the communication is to a machine, not a human, to perform certain tasks, which does add a functional aspect to the software. However, as the court noted, recipes are functional. An extension of the argument is "once language allows one to actually do something, like play music or make lasagna, the language is no longer speech."[86] The ability of one to produce, in other words the functional aspects of speech, should not transform speech to conduct.

The exceptions for printed materials were particularly intolerable to the *Bernstein III* court. The exception distinguished print from electronic publication in an illogical manner.[87] The regulations would allow one to publish Snuffle in a book and distribute it to the far corners of the earth, but publishing on the internet, or on disk, would require an export license.[88]

---

78. *See Bernstein*, 974 F. Supp. at 1292.

79. *See id.* at 1304 (citing Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750, 759 (1988)).

80. *Id.* at 1305.

81. *See id.*

82. *See Bernstein*, 922 F. Supp. at 1434.

83. 491 U.S. 397 (1989) (evaluating the expressive aspects of flag burning in terms of the intent to convey a message and the likelihood the message will be understood).

84. *See Bernstein*, 922 F. Supp. at 1434.

85. *See id.* at 1435.

86. *Id.* at 1436.

87. *See id.*

88. *See id. See also* Karn v. United States Dep't of State, 925 F. Supp. 1 (D.D.C. 1996). A San Diego software developer asked the State Department whether a license was required to export a book illustrating encryption algorithms and providing examples. *See id.* at 3. The

Granted, the effect of this is to require more skill in reducing published material in book form to functioning software. Be that as it may, the stated purpose of the regulations is to protect national security. Those who would harm the national security of the United States would likely be most willing to expend the resources to acquire that skill. In effect this is a law punishing the lawful, while having little or no effect on the lawless. After these rulings, Professor Bernstein was free to teach, publish, and post his programs for his students or the public.

B. The *Junger* Decision

Peter Junger, a law professor at Case Western Reserve University Law School, maintained a web site with information on classes that he taught, which included "Computers and the Law."[89] The instant case made its way to the courts because the plaintiff wanted to post encryption programs in an effort to explain how they work.[90] In compliance with the regulations, the plaintiff submitted applications for commodity classifications.[91] The Commerce Department classified four of the five items as ECCN 5D002.[92]

In *Junger v. Daley,*[93] the plaintiff claimed that the Export Administration Regulations violate the First Amendment[94] because the licensing requirements on the export of encryption technology serve as a prior restraint in violation of the free speech clause of the First Amendment.[95] Additionally, the plaintiff alleged that the regulations are unconstitutional because they discriminate on the basis of content by subjecting some encryption software to more stringent regulations than other encryption software.[96] The government countered that the licensing requirements are only intended to restrict the export of the

---

book is in the public domain and not subject to licensing. *See id.* However, when Karn asked whether a computer disk version required a license, he was informed that the disk was subject to licensing. *See id.* In the author's opinion, this is a distinction without a difference.

89. *See Junger*, 8 F. Supp. 2d at 713-14.

90. *See id.* As noted previously, posting to the Internet would be considered exporting for purposes of the controlling regulations.

91. *See id.*

92. *See id.* The first chapter of Junger's textbook was classified as material that could be exported without a license. Recall ECCN 5D002 allows for encryption of confidential information and the software includes source code and object code among other things. *See also supra* Section III (B).

93. *Junger*, 8 F. Supp. 2d at 711.

94. *See id.*

95. *See id.* at 718.

96. *See id.* at 720-21. The regulations discriminate in the following ways: based on media in that printed forms are exempted; based on the type of software as desktop publishing software is not regulated; and based on strength because fifty-six bit or less encryption is not regulated. *See id.*

software itself, not the idea of encryption.[97] The government requested the district court to review the regulations as content neutral.[98] This request is inapposite to the stated purpose of the regulations, which is to stop the spread of software that can encrypt data. The stated purpose of the regulation is precisely because of the content. However, in the end, the court did view the regulations as content neutral.[99]

The court addressed the question as "whether encryption source code is sufficiently expressive to merit heightened First Amendment protection . . . [and] . . . whether the [regulations] are a prior restraint on speech subject to greater First Amendment scrutiny."[100] The conclusion that the regulations are constitutional is based on the view that encryption source code is inherently functional, the regulations are not directed at expressive elements, and the regulations do not reach academic discussions of software in print form.[101]

First, and most important, the court dealt with whether the encryption source code is sufficiently expressive to merit First Amendment protection. According to the Ohio District Court, encryption source code is inherently functional, enabling a computer to do a designated task.[102] The court's theory is that software is indistinguishable from hardware dedicated to encryption in that encryption software carries out the function of encrypting.[103] The conclusion from this theory is that encryption source code "is exported to transfer functions, not to communicate ideas."[104] The court quickly dismissed the *Bernstein* court's characterization that "language equals protected speech."[105] The operative analysis given for First Amendment protection is whether something expresses ideas.[106] Citing *City of Dallas v. Stanglin*,[107] the

---

97. *See id.* at 711.

98. *See id.* at 710. The test for determining whether a regulation should be reviewed as content neutral is whether the government adopted the restriction because of the views expressed. *See* Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 643, *reh'g denied*, 512 U.S. 1278 (1994).

99. *See Junger*, 8 F. Supp. 2d at 720. The court did not consider that the regulations were passed to suppress disfavored expression. *See id.*

100. *Id.* at 712.

101. *See id.*

102. *See id.* at 712.

103. *See id.*

104. *Junger*, 8 F. Supp. 2d at 716. The court concluded that the exporting of encryption technology is like an encryption device and the value received is the ability of the function the source code provides. *See id.*

105. *Id.* The court disposes of Bernstein by stating that speech is "not protected simply because we write it in a language." *Id.*

106. *See Junger*, 8 F. Supp. 2d at 716-17. The court stated that source code is purely functional in a way that recipes and do-it-yourself manuals are not. *See id.* at 717 (citing Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1997)).

107. 490 U.S. 19, 25 (1989).

Court concluded 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."[108]

The question now becomes whether the Export Administration Regulations act as a prior restraint on speech by requiring review prior to publication and licensing.[109] In order to hold that a licensing law works as a prior restraint on speech, the speech must "have a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of censorship."[110] Again relying on the determination that encryption source code is purely functional, the law was held constitutional.[111] The view espoused was that the expression accompanying the source code and academic discussions describing the software in print media are not regulated and that the non-expressive conduct may be regulated as purely functional.[112]

The court employed an intermediate level of scrutiny to judge constitutionality.[113] The test adopted was that of *Ward v. Rock Against Racism* [114] which consists of determining whether the government-imposed restrictions are based on disagreements with the message.[115] If so, the regulations are content based. If, however, the regulations are implemented without reference to content, they are deemed content neutral.[116] The court stated that the regulations are content neutral because they were imposed without reference to any particular views expressed in the software.[117]

---

108. *Junger*, 8 F. Supp. 2d at 717. *See also* Spence v. Washington, 418 U.S. 405 (1974) (per curiam). *Spence* established guidelines for determining if expressive conduct is "sufficiently imbued with [the] elements of communication to fall within the scope of the First . . . Amendment[]. . . ." *Id.* at 409. The guidelines are whether there is an intent to convey a particular message and the likelihood must be great that those who view the message will understand it. *See id.* The *Junger* Court claimed that encryption source code exportation does not convey a particular message, and that it is designed to be purely functional. *See Junger*, 8 F. Supp. 2d at 716.

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

110. *Id.* (citing City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 759 (1988)).

111. *See Junger*, 8 F. Supp. 2d at 718. The court did not view encryption as integral to expression. *See id.*

112. *See id.* at 718-19. The non-expressive conduct alluded to here is the encryption program source code.

113. *See id.* at 720. The court decision to employ intermediate scrutiny is based on the view that the regulations are content neutral. *See id.*

114. 491 U.S. 781 (1989).

115. *See id.* at 791.

116. *See Turner*, 512 U.S. at 643.

117. *See Junger*, 8 F. Supp. 2d at 720. The government implemented the regulations precisely because of the expressions contained therein. *See id.* To get around this, the *Junger* Court stated that the regulatory distinction is based on the ability of the software to actually perform the function of encrypting data. *See id.* The Court, elaborating on the content neutral distinction, states that the public flow of information in printed form is not restricted. *See id.* As to the distinction between printed form and computerized form on computer disk, the Court

Finally, the plaintiff alleged that content-based discrimination existed because different levels of encryption strength were regulated differently.[118] The court admitted that the government was indeed discriminating based on content. The argument in support of such discrimination is that the regulations are tailored to exports that have long, indecipherable key lengths making them a greater risk to national security.[119]

The application of intermediate scrutiny to determine if content-neutral regulations pass constitutional muster is elucidated in *United States v. O'Brien*.[120] The first prong of the four-part test involves determining if the government's interest is unrelated to the suppression of free expression.[121] The court concluded that the regulations do not limit the free exchange of ideas about encryption, but the government regulates encryption software for the functional ability.[122]

The second prong of the *O'Brien* test states that the regulation should be tailored to further an important or substantial government interest.[123] The court held the important interest prong sufficient because the government's concern for controlling exports that may harm national security is a legitimate one.[124] Obviously, without the regulations, producers of encryption software could export to any person at home or abroad regardless of hostility to the United States.[125] The court stated that the availability abroad of similarly strong encryption software does not diminish the government's interest.[126]

The regulations must also be narrowly tailored to further a substantial governmental interest in order to satisfy the third prong of the *O'Brien* test.[127] Quoting *Ward v. Rock Against Racism*,[128] the court explained that a regulation

---

states that there is a functional difference. *See id.* In printed form, encryption source code is descriptive, while on computer disk, encryption source code can direct a computer to perform a task. *See id.*

118. *See Junger*, 8 F. Supp. 2d at 721. *See also* 15 C.F.R. § 742.15(b)(1)-(2) (1996) (stating that encryption of low key strength is not covered under the regulations).

119. *See Junger*, 8 F. Supp. 2d at 721. (noting that the content discrimination is ancillary to the discrimination based on functionality, and, therefore, not directed at the content of ideas).

120. 391 U.S. 367, 377 (1968) (dealing with symbolic speech upholding conviction of one who burned his draft card because it frustrated legitimate government interests).

121. *See id. See also* Texas v. Johnson, 491 U.S. 397, 406 (1989) (stating that a law may not prohibit specific conduct to reach its expressive elements).

122. *See Junger*, 8 F. Supp. 2d at 722 (coming to this conclusion for the same reason it concluded that the regulations are content neutral—it is the regulation of the function of the software, not the free exchange of ideas about encryption).

123. *See O'Brien*, 391 U.S. at 377.

124. *See Junger*, 8 F. Supp. 2d at 721-22.

125. *See id.* at 722.

126. *See id.*

127. *See O'Brien*, 391 U.S. at 377.

128. *Ward*, 491 U.S. at 799.

must not "burden substantially more speech than is necessary to further the government's legitimate interests."[129] This explanation does not say the regulation must make it harder for someone to express, or achieve, something in order for it to be narrowly tailored. Yet, that is what the court apparently relied on when it stated, "[e]ncryption software posted on the internet or on computer diskette can be converted from source code into workable object code with a single keystroke."[130] The identical matter, the court conceded throughout, may be legally exported when published in text format. Therefore, someone with the technical ability to understand source code on disk has the same understanding of material in print.

The last prong of *O'Brien* consists of determining whether the regulations burden more speech than is necessary to further the government's interests.[131] As a determining fact, the court states that short key encryption needs no license for export in an attempt to demonstrate that the export controls are targeted at the specific activity threatening legitimate government interests.[132] A supporting consideration given by the court was that printed form encryption is not reached by the regulations.[133] Finally, the court noted that the regulations leave alternative channels of communication open,[134] and therefore satisfy intermediate scrutiny.[135]

C. Discussion

Both the *Bernstein* and *Junger* cases carry great import for the future of private communications on the internet. However, both cases leave gaps in the analysis of encryption software source code. *Junger* almost wholly discounts the expressive elements of encryption source code and the content based discrimination of the government regulations. *Bernstein* did discuss the functional aspects of encryption source code, but left many important questions unanswered. The remainder of this comment will discuss some of the issues left unresolved and then review the Constitutional implications and proposed legislative bills.

---

129. *Junger*, 8 F. Supp. 2d at 722.

130. *Id.* The effect of this is to make someone put the printed text on disk, which hardly satisfies the admonition in *Ward* that the narrowly tailoring requirement is satisfied if the government's interest would be "achieved less effectively absent the regulation." *Ward*, 491 U.S. at 799.

131. *See O'Brien*, 391 U.S. at 377.

132. *See Junger*, 8 F. Supp. 2d at 723.

133. *See id.*

134. *See id.* (citing *Ward*, 491 U.S. at 802).

135. *See id.* The Court stated, "[b]ecause the content neutral export regulations at issue enable the government to collect vital foreign intelligence, are not directed at a source code's ideas, and do not burden more speech than necessary, they satisfy intermediate scrutiny." *Id.*

The *Bernstein* court used analogies to music, foreign languages, and do-it-yourself manuals to discount the functional capacity of encryption source code. Source code is translated to object code by interpreter software so that it may instruct a computer to do specific tasks. Some would argue this use is purely functional. The music analogy is instructive, though not determinative, in that music contains instructions to a human to perform certain tasks. Similarly, a recipe is functional in that it is instructive, not expressive. Encryption, however, contains instructions to a computer and not a human to independently perform some task. The court does not discuss this distinction. The instructions are purely functional, focusing on how to develop encryption, not what rhetoric to use. This purely functional aspect should not transform highly protected speech to conduct open to regulation. For example, desktop publishing software could not be restricted in its use in the name of order. The software would be purely functional, yet the software is indisputably a medium of expression. These problems will have to be solved as computers permeate every aspect of our lives.

Copyright law can assist in some fashion. Copyright is the protection of the expression of ideas. Legal scholars could argue that encryption is the idea and that source code is the expression of that idea, which is subject to copyright protection. Assuming that copyright protection is attainable, it remains to be seen whether that would be enough to conclude source code expression. The answer remains to be seen.[136] The concern with the *Bernstein* analysis is the narrow scope, focusing on the nature of source code as language, and, therefore, speech.

The *Junger* court's analysis is deficient in regard to encryption source code as expressive speech, content-based discrimination, and the realities of the present university environment. The *Junger* analysis does not acknowledge that encryption is a course of applied mathematics taught at many universities. The purpose is to utilize algorithms to create other modes of communication. The government asserts this is not a language but a function, akin to placing a letter in an envelope so that no one can get the information. However, encryption source code is more like a foreign language than a hardware device, and the Supreme Court has afforded foreign languages protections from government prohibitions.[137] People familiar with source code and encryption algorithms can understand and debate the merits of the language. Without the

---

136. Judge Patel, in *Bernstein I*, reasoned that encryption expressed in source code communicates how to make the idea of encryption functional, and, as a result, copyright law supports source code as a means of expression. *See Bernstein I*, 922 F. Supp. at 1436.

137. *See* Yniguez v. Arizonans for Official English, 69 F.3d 920, 936 (9th Cir. 1995), *vacated on other grounds*, 520 U.S. 43 (1997) (concluding that speech in any language is speech).

source code, there could be no expression of the idea of encryption. The regulations restrict the use and teaching of an idea, encryption, in a way that makes certain expression illegal. Thus, the expression of the idea of encryption should be afforded heightened First Amendment protection.

The *Junger* analysis also falls short in concluding the regulations are content neutral. The government's concern is the recipient's ability to encrypt data. Clearly, this has functional *and* content-based implications. The restriction is imposed precisely because of the content, which allows the function of encryption. The licensing is aimed at the export of a particular aspect of a particular computer language. This would seem to fail the test of *Texas v. Johnson* in disallowing prohibitions on conduct (exporting) to get to expression (encryption source code). To simplify matters, the regulations restrict only algorithms and software associated with encryption, but not other types. This quintessential content-based restriction is aimed at suppressing the expression of an idea that the government deems to be dangerous. This aspect alone should trigger the strongest First Amendment protections; however, *Junger* applied the lenient symbolic speech test of *O'Brien*. The question that must be answered involves why we would restrict cyberspeech in a way that we would not restrict other forms of speech. This question implicates a form of discrimination that requires the more stringent standards of *New York Times Co. v. United States.*[138]

Finally, *Junger* does not acknowledge the realities of modern day universities. The Court states that textual and printed versions of the encryption source code are not limited by the regulations and, therefore, the regulations are Constitutional. However, many foreign students attend classes in the United States. Many professors maintain web sites to post class information and syllabi. So, *Junger* does not resolve the plaintiff's dilemma in that talking to a foreigner about encryption, teaching encryption in a class with foreigners, or placing problem sets of algorithms on the internet are all prohibited by the plain language of the regulations.[139]

These cases, though furthering the debate, are short on comprehensive analysis of all necessary factors and a realistic view of the current technological environment. Citizens concerned with liberty and privacy interests are worried these cases leave too much to chance for future internet communications. Lobbying and television advertising campaigns have begun to push Congress to enact strong encryption legislation. The next sections will review some of the legislative proposals and the Constitutional implications.

---

138. 403 U.S. 713 (1971) (stating that prior restraint of speech is only justified when disclosure results in direct, immediate, and irreparable harm).

139. *See* discussion *supra* Section III.

V. PROPOSALS

A. Security and Freedom Through Encryption Act, H.R. 695, 105th Cong. (1998)

One of three major proposals to promote privacy and security on the Internet, the Security and Freedom through Encryption Act (SAFE)[140] has solid bi-partisan support in the House of Representatives.[141] Many devoted to liberty and privacy favor this bill for many reasons. First, the bill affirms the freedom to use or sell the strongest available encryption.[142] Next, the bill defeats any governmental attempts at mandatory key recovery systems.[143] Finally, the bill allows American companies to compete with foreign companies in the encryption market by lifting all export regulations on encryption software.[144] Americans for Computer Privacy, an advocacy group, reports that the bill has wide support from the financial services industry, the health care industry, privacy groups, the high-tech community, and both liberal and conservative think tanks.[145]

B. The E-Privacy Act, S. 2067, 105th Cong. (1998)

The E-Privacy Act[146] is aimed at fostering privacy on the Internet.[147] The bill is proposed to fulfill eight goals.[148] First, the bill seeks to preserve the right to choose the method of protecting private communications and information.[149] Most significant to liberty proponents is that the bill also bars government

---

140. Sponsored by Representatives Bob Goodlatte, a Republican from Virginia, and Zoe Lofgren, a Democrat from California.

141. *See* Americans for Computer Privacy, *Computer Privacy; Bills in Congress* (visited July 15, 1998) <http://www.computerprivacy.org/bills> (focusing efforts on computer privacy rights).

142. *See Secure Public Networks Act* (visited July 15, 1998) <http://thomas.loc.gov /cgi-bin/query/D?c105:2:./temp~c105Az2GTT:e37986>. Section 2802 states in relevant part: ". . . it shall be lawful for any person within any State, and for any United States person in a foreign country, to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used." *Id.*

143. *See id.* Section 2804 states in relevant part: "PROHIBITION-No person in lawful possession of a key to encrypted information may be required by Federal or State law to relinquish to another person control of that key." *Id.*

144. *See id.*

145. *See supra* note 141.

146. Sponsored by Senators John Ashcroft and Conrad Burns, Republicans from Missouri and Montana, respectively, and Senator Patrick Leahy, a Democrat from Vermont.

147. *See supra* note 141.

148. *See Congressional Record Statement* (visited July 8, 1998) <http://www.senate.gov/~leahy/s980512.html>.

149. *See id.*

mandated key recovery encryption systems.[150] The third goal establishes both procedures and standards for law enforcement access to decryption keys for both encrypted communication and stored electronic data, permitting access only upon proper authority and procedural safeguards.[151] Also, the bill establishes standards and procedures for foreign government access to the plaintext of encrypted communications.[152] The last two goals of the bill concern privacy advocates and are largely the reason for more widespread support for the SAFE act. The instant proposal seeks to set up a National Electronic Technology Center (NET Center) to assist law enforcement officials in researching ways to lawfully monitor encrypted communications under proper authority.[153] The final significant goal is to update export controls to guarantee competition in the global marketplace by American companies that are now, in effect, shut out.[154] Due to concerns that the Net Center would create a new bureaucracy with the potential to infringe liberty, this bill does not have the widespread support that the SAFE act enjoys.[155]

C. The Secure Public Networks Act, S. 909, 105th Cong. (1998)

The last significant proposal, The Secure Public Networks Act, is very similar to what the Clinton Administration and the FBI have been putting forth since the inception of this debate.[156] This proposal is very similar in relevant aspects to the current regulatory scheme. In addition, the bill would require every American utilizing encryption to deposit a spare key in government-approved third party accounts. For this reason, liberty and privacy advocates have not supported this bill.

VI. CONSTITUTIONAL IMPLICATIONS

One should consider the Congressional proposals and current regulations in light of their Constitutional implications. Any system of mandatory key

---

150. *See id.*
151. *See id.*
152. *See id.*
153. *See supra* note 141.
154. *See Congressional Record Statement* (visited July 8, 1998) <http://www.senate.gov/~leahy/s9805.html>.
155. *See* Center for Democracy and Technology, *Senators introduce pro-privacy encryption . . . Administration Position* (visited July 10, 1998) <http://www.cdt.org/press/051298press.htmlh>. The Center for Democracy and Technology believes the provisions may create new burdens on privacy.
156. Sponsored by Senator John McCain, a Republican from Arizona, and Senators Bob Kerrey, John Kerry, and Ernest Hollings, Democrats from Nebraska, Massachusetts, and South Carolina, respectively.

escrow necessarily implicates the Fourth and Fifth Amendments to the Constitution. The *Bernstein* and *Junger* cases analyzed the implications for the First Amendment to the Constitution, but not to the extent or satisfaction of advocates on both sides of the debate. The free flow of communication—from credit card transactions to e-mail critical of government—has been a sensitive matter for Americans since the inception of our nation.[157] The basic value of private communication is as important today as it has ever been, and encryption allows for that private communication. There are costs, however, such as limiting law enforcement's ability to monitor and evaluate the communications of dangerous criminals and terrorists. It is understandable that law enforcement officials would propose mandatory key escrow for easy, immediate access to internet communications. However, the question is whether law enforcement's legitimate interest in monitoring terrorists and criminals may justifiably curtail the liberty and privacy interests of the First, Fourth, and Fifth Amendments.

A. The First Amendment

The First Amendment provides in relevant part that "Congress shall make no law abridging the freedom of speech, or of the press."[158] The First Amendment is not absolute, but has been applied to numerous mediums.[159] With regard to academics, the Supreme Court has stated that the imposition of a "strait jacket" on academic leaders in universities imperils the future of the nation.[160] Of course, some speech may be restricted, such as shouting "fire" in a crowded theater.[161] The Supreme Court, however, insists that entire categories of speech may not be subject to prior restraint or categorically regulated.[162] The mandatory key escrow proposals and licensing requirements contravene these First Amendment principles by placing a ban and prior restraint on a medium of expression that academics utilize.

---

157. During the debates on the Constitution, writers used pseudonyms to protect their identity when conducting public debate through newspapers. *See generally The Federalist Papers.*

158. U.S. CONST. amend. I.

159. *See* CBS v. Democratic Nat'l Comm., 412 U.S. 94 (1973) (applying first amendment to broadcasting medium); United States v. Paramount Pictures, Inc., 334 U.S. 131 (1948) (applying first amendment to motion pictures, radio, and newspaper mediums); Lovell v. City of Griffin, 303 U.S. 444 (1938) (applying first amendment to leaflets as a medium).

160. *See* Sweezy v. New Hampshire, 354 U.S. 234, 250 (1957). The Attorney General of New Hampshire petitioned a state court to propound questions regarding a university lecture to plaintiff who was held in contempt for repeated failure to answer. *See id.*

161. *See* Schenk v. United States, 249 U.S. 47 (1919).

162. *See* Brandenburg v. Ohio, 395 U.S. 444 (1969) (stating absent obscenity, extortion or blackmail, the government is required to prove its case that an instance of speech is likely to cause sufficient harm to justify the regulation).

Encryption is a recognized science taught at many universities around the country. The idea is encryption and the expression of that idea is the algorithms constituting encryption source code. The argument in *Junger* is that encryption is not speech because it is purely functional.[163] However, chemical equations and recipes are purely functional mediums of expression, which are protected.[164] The lack of familiarity with a particular language should not, of itself, strip that language of protections afforded speech.[165] Therefore, source code, as a form of expression, should be afforded the same protections a foreign language, recipe, or chemical equation is given. The caveat, carved out in *Brandenburg*,[166] is that all expression should be permitted, unless evidence exists that particular forms of speech cause serious harm.[167]

The *Junger* court accepted the argument proposed by advocates of encryption regulations that source code is not sufficiently expressive to merit First Amendment protections. The activities at issue are considered conduct in the same way that stuffing envelopes with letters, moving one's lips to speak, or utilizing a printing press to mass produce leaflets are considered conduct. These are classic cases of mediums of expression falling within the ambit of the First Amendment. Accepting the expressive conduct contention would call for application of the more lenient intermediate scrutiny revealed in *O'Brien*.[168] However, the more recent case of *Yniguez v. Arizonans for Official English*[169] asserted that all speech can be viewed as expressive conduct and fall under intermediate scrutiny.[170] Language, by definition, is speech, and so the regulation of language is the regulation of speech.[171]

Accepting the *O'Brien* test does not necessarily lead us to the same conclusion that the *Junger* Court announced. The government argued that the regulations are aimed not at the expression, but the functional use of encryption source code. This argument fails to recognize that the unregulated printed form of expression is every bit as functional to a mathematician as the same information on computer disk. Similarly, one who cannot distinguish source code from any other computer language will not be helped by that information being on disk. It appears that the government wishes to limit the ready

---

163. *See Junger*, 8 F. Supp. 2d 708.
164. *See Bernstein*, 922 F. Supp. at 1435-36.
165. *See Yniguez*, 69 F.3d at 936.
166. *See Brandenburg*, 395 U.S. at 444.
167. *See id.*
168. *See O'Brien*, 391 U.S. at 367.
169. *See* Yniguez v. Arizonans for Official English, 69 F.3d 920 (9th Cir. 1995), *vacated on other grounds*, 520 U.S. 43 (1997).
170. *See id.* For this reason *Yniguez* "emphatically reject[ed]" the idea that speaking in a foreign language is expressive conduct as opposed to pure speech. *See id.* at 934.
171. *See id.* at 935.

availability of the source code by those who cannot understand the information. This reasoning finds no support in *O'Brien* and, therefore, fails this test.

The mandatory key escrow proposals contravene, among other rights, the right not to speak. Allowing the government unfettered access to secure communications puts us in a position of being forced to speak against our will. The government could reveal our identity through mandatory key access while we engage in constitutionally protected conversations. For example, civil rights activists cannot be compelled to disclose the identity of members or authors of protected pamphlets, journals, or commentary.[172] Internet communications and transactions encrypted by their senders and recipients are encrypted precisely because they seek to keep their identity and comments anonymous.

The current regulatory scheme, and the proposals maintaining those systems, also fail the second prong of the *O'Brien* test. The second prong requires that the regulation further a significant governmental interest.[173] The interest the government puts forth is indeed legitimate and significant. The analysis, however, turns on whether the regulations *further* these significant legitimate interests. The advent of these regulations has seen a dramatic increase in the availability of encryption products imported from foreign corporations and exported from foreign countries to our trading partners.[174] The effect of these regulations is to cripple the domestic encryption technology industry while doing little to improve national security.[175] For this reason, the *Junger* analysis should fail the second prong *O'Brien* by failing to *further* the legitimate interest.

The requirement that the "governmental interest is unrelated to the suppression of free expression" may be regarded as requiring alternative channels of communication.[176] *Junger*, the E-Privacy Act, and the Safe Public Networks Act fail the third prong of the test. The government repeatedly asserts that the printed form of source code is not regulated and, therefore, an alternative channel of communication is available. However, as noted earlier, posting the software to the internet is a violation of the export regulations. This one fact causes the analysis in *Junger* and the congressional proposals

172. *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958). "Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly." *Id.*

173. *See O'Brien*, 391 U.S. at 376-77.

174. *See E-Commerce & Y2K: What's Ahead For Small Business: Hearing Before the United States Senate Committee on Small Business*, 105th Cong. (1998) (statement of Harris N. Miller, President, Information Technology Association of America).

175. *See O'Brien*, 391 U.S. at 376-77.

176. *See id.* at 377. It seems that any regulation suppressing expression that has only one medium of communication would inextricably tie the governmental interest with the expression in violation of the Constitution.

mentioned to fail the third prong of *O'Brien*. The internet is the only alternative able to implement the idea and test the efficacy of any algorithm.

The government regulations and current proposals mandating key recovery have the definite impact of discouraging the open exchange of ideas on the internet, which should trigger strict scrutiny in any First Amendment analysis. The internet communicator would, in essence, live in a glass house. Any proposal, or regulation, that limits key strength is, by definition, content-based discrimination that carries a heightened level of scrutiny under the First Amendment.

Finally, the licensing requirements, which are left to the discretion of the executive branch with no judicial review, work a prior restraint on the free exercise of First Amendment rights. The Supreme Court expressly stated, in *44 Liquormart, Inc. v. Rhode Island,*[177] that "speech restrictions cannot be treated as simply another means that the government may use to achieve its ends."[178] The Supreme Court has also recognized that scientific and academic research is at the core of First Amendment protections.[179] It seems apparent that the gravamen of the argument in favor of encryption restrictions is that regulating this speech will offer temporary safety. This line of reasoning should be considered an open invitation to strike the regulations.[180] For the foregoing reasons, source code should be found to be speech under the First Amendment, key escrow a violation of rights under the First Amendment guarantee of freedom to speak or not speak, and licensing requirements a prior restraint discouraging the free expression of ideas.

B. The Fourth Amendment

The Fourth Amendment to the United States Constitution protects the right of all citizens to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[181] The key recovery proposals were not a part of the *Junger* and *Bernstein* cases, so the focus of this section is on the Congressional proposals[182] to mandate key recovery.[183] The Fourth

177. 517 U.S. 484 (1996).

178. *Id.* at 512.

179. *See* Keyishian v. Board of Regents, 385 U.S. 589, 603 (1967). *See also* Board of Trustees of Leland Stanford Junior Univ. v. Sullivan, 773 F. Supp. 472, 474 (D.D.C. 1991) ("[T]he First Amendment protects scientific expression and debate just as it protects political and artistic expression.").

180. *See* Edenfield v. Fane, 507 U.S. 761 (1993) (stating, in a commercial speech context, that the government may not sustain a regulation on commercial speech without demonstrating that the potential mischief is real and that the regulation will in a particularized way curtail the mischief to a material degree).

181. U.S. CONST. amend. IV.

182. *See supra* Section V. The Safe and E-Privacy proposals prohibit mandatory key

Amendment states that "no warrants shall issue, but upon probable cause" and "particularly describing" the target(s) of the search.[184] However, one of the proposals, The Secure Public Networks Act, allows law enforcement officials to obtain the access to your communications with a more general subpoena, as opposed to a search warrant specifying a particular target for the search.[185] Mandatory key escrow proposals, requiring nothing more than a subpoena without a particularized search target, would easily lead to dragnet searches resulting in a significant infringement on the security and privacy of every individual communicating or transacting business on the internet[186] in violation of Fourth Amendment protections.[187]

The Fourth Amendment protections have continually been modified and extended to address technological advances. In 1967, the Supreme Court held that a warrantless wiretap was equivalent to the British rummaging through eighteenth century papers.[188] The parallels to secure internet communication are patently obvious. One speaking on the telephone inside the home has a reasonable expectation of freedom from warrantless search and seizure. Similarly, one communicating on the internet does so over the telephone line from the same home phone with the same reasonable expectation of privacy. It could be argued that the communication is no different at all than a telephone conversation and key escrow amounts to a wiretap. If, on the other hand, one

---

access; however, the Secure Public Networks Act and Executive Office proposals do require key recovery. *See supra* Section V.

183. *See* Richard R. Mainland, *Congress Holds the Key to Encryption Regulation*, NAT'L .L.J., Apr. 20, 1998, at B9. The FBI and other law enforcement agencies have argued strongly that encryption manufacturers require key recovery so that they can penetrate the plaintext messages without the knowledge of the parties to the communication. *See id.*

184. *See* U.S. CONST. amend. IV. The reason for this amendment is undoubtedly to curtail dragnet searches that trap numerous innocent citizens in their everyday activities, which would greatly harm the privacy of lawful citizens. *See Privacy in the Digital Age: Encryption and Mandatory Access, 1998: Hearings before the Subcommittee on the Constitution of the Senate Committee on the Judiciary,* 105th Congress (1998) (statement of Kathleen M. Sullivan, Professor, Stanford Law School).

185. *See Secure Public Networks Act*, §106(2)(a) (visited July 15, 1998) <http://thomas.loc.gov/cgi-bin/query/D?c105:1:./temp/~c105Vfj6fo:e988:>. "A key recovery agent, whether or not registered by the Secretary under this Act, shall disclose recovery information: (a) To a government entity if that entity is authorized . . . or obtained . . . a subpoena authorized by Federal or State statute . . . ." *Id.*

186. *See Privacy in the Digital Age: Encryption and Mandatory Access, 1998: Hearings before the Subcommittee on the Constitution of the Senate Committee on the Judiciary,* 105th Congress (1998) (statement of Kathleen M. Sullivan, Professor, Stanford Law School).

187. *See* Stanford v. Texas, 379 U.S. 476 (1965) (invalidating a search warrant authorizing the search of a home for books, records, and other materials relating to the Communist Party, on the ground that the warrant authorized law enforcement officials to rifle through and make discretionary judgments about books and records that is in effect the equivalent of a general warrant, one of the primary targets of the Fourth Amendment).

188. *See supra* note 186 (citing Katz v. United States, 389 U.S. 347 (1967)).

argues e-mail is more like a letter, that argument also fails. One who sends a postcard does not have a reasonable expectation of privacy.[189] However, place that same postcard in an envelope and there is a reasonable expectation of freedom from warrantless search and seizure. Courts may easily analogize encryption software to an envelope's purpose of concealing confidential contents. Certainly, the government could not restrict the use of gummed envelopes to facilitate the monitoring of potential domestic or foreign terrorists. That is the essence of mandatory key recovery proposals, which turn historical Fourth Amendment presumptions upside down by requiring citizens to assist law enforcement officers in the surveillance of private communications.[190] There is no difference between mandating key escrow for encryption software and mandating key escrow to our homes. Both could be supported by the argument that national security is at risk, and the government needs ready access to potential criminal's homes. Similarly, the government could not outlaw locks, or mandate the escrow of keys to gun cabinets with a third party to easily track the number of shotguns citizens keep. Suppose our medical records or bank statements are encrypted on computer diskettes. The IRS would not be able to demand the keys to our computer files under the authority of a subpoena without violating the Fourth Amendment. There is no difference between that and the government requiring us to keep the hard copies of these records in a government access vault. Suppose the government mandated in home cameras with the promise that they would not turn them on absent suspicion of illegal activity.[191] Again, that does not differ from the monitoring effectuated by mandatory key escrow. All communications on the internet under such a proposal amount to living in a glass house. For the internet to attain its full potential, internet communications must carry the protections afforded traditional speech.

C. The Fifth Amendment

The relevant portion of the Fifth Amendment states that no person "shall be compelled in any criminal case to be a witness against himself."[192] The protections offered by this clause consist of a simultaneously testimonial communication that is incriminating and governmentally compelled.[193] The

189. *See* Oliver v. United States, 466 U.S. 170 (1984) (concluding Fourth Amendment does not preclude law enforcement searches of open areas visible to passers by).

190. *See supra* note 186.

191. *See supra* note 186.

192. U.S. CONST. amend. V.

193. *See Privacy in the Digital Age: Encryption and Mandatory Access, 1998: Hearings before the Subcommittee on the Constitution of the Senate Committee on the Judiciary,* 105th Congress (1998) (statement of Kathleen M. Sullivan, Professor, Stanford Law School).

Fifth Amendment protections are implicated in that, absent mandated key recovery, the government would have to compel disclosure of the encryption key.[194] If the encrypted communication is incriminating, then the disclosure of the key triggers the protection of the Fifth because the government is compelling access to the incriminating testimonial communication.[195] However, mandated key recovery would circumvent the Fifth Amendment protections. While it is true that the key escrow is compelled, any use of the key to decrypt incriminating testimonial communication would be voluntary.[196] For example, assume a criminal defendant is using encrypted e-mail to discuss trial strategy with an attorney. If law enforcement officials use the escrowed key to decrypt the communication, that could lead to self-incrimination. The government would compel the escrow of the key, but the communication is not compelled, and, therefore, presumably would not violate the Fifth Amendment. On the other hand, if there is no mandatory key recovery and officials compel the communication, that would violate the Fifth Amendment. The use of this method to subvert the Fifth Amendment is intolerable to liberty and privacy advocates.

VII. CONCLUSION

The internet has tremendous potential to improve productivity, facilitate business transactions, and improve many other aspects of everyday life. Encryption technology is a way of maintaining the liberty and privacy interests of the Constitution. The notion that encryption is inherently functional, and thus conduct, runs counter to the numerous mediums held subject to First Amendment protections. Business and consumer confidence in the Internet depends upon privacy protection. To ensure that our nation moves down the path of liberty to the future of the information age, Congress must pass legislation to protect security on the internet and lift the existing regulations on encryption technology. So, Mr. Henry, what say you to Mr. Franklin? Liberty, or temporary safety?

Forbid it, Almighty God! I know not what course others may take, but as for me, give me liberty, or give me death!

Patrick Henry

Joe Baladi

194. *See id.*

195. *See id.*

196. *See id.* Even if the enabling encryption is incriminating to the user, it is not incriminating testimony by the third party escrow agent holding the key. *See id.*