Maryland Journal of International Law

Volume 22 | Issue 2 Article 6

An Overview of the Issues Surrounding the Encryption Exportation Debate, Their Ramifications, and Potential Resolution

E. Franklin Haignere

COMMENT

AN OVERVIEW OF THE ISSUES SURROUNDING THE ENCRYPTION EXPORTATION DEBATE, THEIR RAMIFICATIONS, AND POTENTIAL RESOLUTION

I. INTRODUCTION

Historically, encryption has been a contest between the "coders" and the "decoders."[1] While in the past encrypted messages have been decrypted with varying degrees of success, it is now possible with modern mathematical algorithms to encrypt messages that without the proper keys are, for all practical purposes, impossible to crack.[2] This situation ensures the secrecy of military intelligence and also provides important benefits to those who own such intellectual property as movies or audio recordings, to financial institutions who want to exchange information electronically, and to a vast array of corporations and individuals who want to maintain their proprietary knowledge or trade secrets.[3] Unfortunately, strong encryption also brings with it the opportunity for misuses such as terrorism, fraud by organized crime, and spying.[4] These potential

---

1. "Encryption" is the process by which the original text of a message, which is known as "plaintext" and can be read by humans, is transformed into a text known as "ciphertext" that the sender and recipient intend to be unintelligible to third parties. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 1 (1994). "Decryption" is the reverse process of encryption that transforms the ciphertext message into the original plaintext. *Id.* The transformation process is accomplished through the use of mathematical algorithms and keys. *Id.* at 2. The strength of an encryption program is determined by the length of its key and the complexity of its algorithm. *Id.* at 129. Key lengths are measured in bits. *Id.* Each bit is equal to a binary digit (either 0 or 1) and every additional bit doubles the strength of the encryption. *Id.* at 2, 129. So a 128-bit key would require that all 128-bits be correct before the message could be decrypted and is twice as strong as a 127-bit key.

2. *Id.* at 7. Using existing technology anyone willing to spend $100,000 would be able to break a 40-bit key in 2 seconds; a 56-bit key in 35 hours; a 64-bit key in 1 year; an 80-bit key in 70,000 years; a 112-bit key in 10\]14 years; and a 128-bit key in 10\]19 years. Jim Kerstetter, *Key Uprising*, PC WEEK, Sept. 29, 1997, at 1, 18, *available in* 1997 WL 12481899.

3. Ira S. Rubinstein, *Export Controls On Encryption Software*, *in* COPING WITH U.S. EXPORT CONTROLS 1996, at 309, 311 (PLI Com. Law and Practice Course Handbook Series No. A4-4512, 1996).

4. *See, e.g.*, Note, Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 496 (1996). See Terrence Stender, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 CASE W. RES. J. INT'L L. 287 (1998), for a discus-

misuses have prompted the federal government to enact laws regulating encryption.[5] But while attempting to address these misuses, the current regulations place too many restrictions upon U.S. companies and reasonable uses and sometimes produce results which are neither logical nor sensible. Complicating the situation are the decisions that have been handed down by three federal district courts, which are divided as to the constitutionality of the current export regulations in regards to the First Amendment. Meanwhile, within Congress and the Executive Branch there is an ongoing debate about whether the current regulations should be relaxed, and if so, to what degree.

Moreover, while the current U.S. encryption export controls may promote legitimate government ends, if they are ultimately to be effective, they must be part of a larger international system. Any unilateral action taken by the United States is unlikely to be successful due to the nature of encryption, the ease with which it can be produced and transported, and the rapid advances occurring in computer technology. This comment details and analyzes the current export regulations, how the current U.S. controls are being circumvented, the applicable case law, and some of the proposed reforms as well as how other nations limit the exportation of encryption while concluding with a suggested course of action.

II. CURRENT ENCRYPTION REGULATIONS

Although the import, sale and use of encryption products within the United States is legal, the exportation of these same products is subject to government control under the Export Administration Regulations (EAR).[6] The Bureau of Export Administration (BXA) has regulatory ju-

---

sion of the importance of national security in the encryption debate.

5. Louis Freeh, the Director of the FBI, in testimony before the U.S. Senate Judiciary Committee's Technology, Terrorism, and Government Information Subcommittee, stated that without a national policy on encryption, "our ability to investigate and sometimes prevent the most serious crimes and terrorism will be severely impaired." Bill Pietrucha, *Computer Industry to Press for Encryption Relief*, NEWSBYTES NEWS NETWORK, Feb. 25, 1998, *available in* 1998 WL 5030256.

6. Export Administration Regulations, 15 C.F.R. Pt. 730-740 (1998). *See, e.g.*, CARL MIDDLEHURST, ET AL., *Collection of Articles by Carl Middlehurst of Sun Microsystems, Inc, in* 17TH ANNUAL INSTITUTE ON COMPUTER LAW: THE Evolving Law of the Internet Commerce, Free Speech, Security, Obscenity and Entertainment, at 549, 553 (PLI Patents, Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. G4-3987, 1997). The reasoning according to the EAR is that "encryption items can be used to maintain the secrecy of information, and thereby may be used by persons abroad to harm national security, foreign policy and law enforcement interests." 15 C.F.R. §742.15 (1998).

risdiction over the encryption items and activities that are subject to the EAR.[7] The encryption items that are subject to the EAR are defined as all encryption commodities, software, and technology that contain encryption features.[8] Any individual or company that wants to export materials containing encryption strength of over 56-bits from one of these three categories in compliance with the regulations must submit an export license application to the Department of Commerce.[9] These licenses are required for the exportation of encryption items to all destinations except Canada.[10] The BXA then reviews each application for a license on a case-by-case basis and determines "whether the export or reexport is consistent with U.S. national security and foreign policy interests."[11]

The encryption regulations that were in place until September, 1998, permitted the granting of licenses for non-recovery encryption items that used key lengths of up to 56-bits if they were accompanied by a commitment to develop recoverable items. Without such a promise licenses were to be granted only for 40-bit key lengths.[12] Though by demonstrating that

---

7. 15 C.F.R. §734.2(a)(1) (1998).

8. *See* 15 C.F.R. §772 (1998).

9. 15 C.F.R. §742.15(a) (1998). *See White House Statement on Administration Encryption Policy*, U.S. NEWSWIRE, Sept. 16, 1998, *available in* 1998 WL 13605470 (announcing the increase to 56-bits the encryption strength that can be exported without a license) (hereinafter *White House Statement*). *See also Transcript of White House Press Briefing on Encryption*, U.S. NEWSWIRE, Sept. 16, 1998, *available in* 1998 WL 13605481 (hereinafter *White House Briefing*). *See infra* text accompanying notes 14-15.

10. 15 C.F.R. §742.15(a) (1998). Canada is excepted from these license requirements because under bilateral agreements Canada respects certain U.S. export controls and will not ship U.S. origin goods to certain countries without appropriate U.S. export licenses or verification that the specified goods may be exported to that specified country without the U.S. license, and even then only after the issuance of an individual Canadian export permit. Andrea F. Rush & Lisa R. Lifshitz, *A Canadian Perspective on International Licensing, in* LICENSING AGREEMENTS 1998, at 375-76 (PLI Pat., Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. G4-4033, 1998) (citing s. 2 of GEP No. 12, SOR/97-107). The U.S. encryption regulations do not allow licenses to be granted for exports to Cuba, Libya, North Korea, Iraq, Iran, Syria and Sudan. 15 C.F.R. §740.8(c) (1998).

11. 15 C.F.R. §742.15(b) (1998).

12. 15 C.F.R. §742.15(b)(3) (1998). Normally encryption is designed to only permit the sender and the receiver of the encrypted message to know the "key" that will allow the message to be decrypted. Key recovery encompasses a variety of techniques that would enable third parties, such as law enforcement agencies, to also obtain the key and decrypt the message. This enables keys to be "recovered after they have been lost, maliciously destroyed, or intentionally withheld." *Cylink: U.S. Government Licenses Cylink to Export the Triple-DES Encryption Algorithm World-Wide*, M2 PRESSWIRE, May 18, 1998, *available in* 1998 WL 12206778 (hereinafter *Cylink*).

it could already deliver key recovery, a company could apply for a license that would permit the exportation of key lengths of up to 128-bits.[13] However, on the sixteenth of September, 1998, the Clinton administration officially loosened its position on what level of encryption was consistent with national security by making an announcement that created a new policy regarding encryption exportation that became effective immediately.[14] The new policy allows for the export of key lengths of 56-bits or less without a license and without a promise to develop key recovery after a one-time technical review.[15] Products containing encryption with key lengths of over 56-bits can not be exported unless they fall under one of the exceptions.[16]

A. *Exceptions That Have Been Permitted*

There are normally several exceptions to the EAR's general export licensing framework, but only some of these are available to products containing encryption. For example, technology or software products that either are already publicly available or contain a de minimis level of U.S. parts normally come within an exception to the EAR.[17] However, products that contain encryption are not eligible for these exceptions.[18] Nevertheless, in what seems like a contradiction to the above policies, phono graphic records and most printed matter containing encryption are not subject to the EAR.[19] This often results in the printed form of an encryption program being exportable, while the electronic version is not.[20]

---

13. *See* 15 C.F.R. §740.8(b)(1) (1998).

14. *See White House Statement, supra* note 9 (stating that the new policy "supports law enforcement and national security" and that it "will protect our national security and our safety.")

15. *Id.* In the same announcement the administration also extended an exception that had originally been created for financial institutions to insurance, medical, and health-care companies. *Id.* See *infra* text accompanying note 31.

16. *Id.*

17. 15 C.F.R. §734.7(c) (1998) (publicly available exception). 15 C.F.R. §734.3(b)(3) & 734.4 (1998) (de minimis exception).

18. 15 C.F.R. §732.2(b) & (d), 734.3(b)(3), 734.4(b) (1998).

19. 15 C.F.R. §734.3(b)(2) (1998). Encryption source code that is in electronic form or media, such as a computer diskette or CD ROM, is still subject to the EAR. 15 C.F.R. §734.3(b)(3) (1998).

20. *See* Bernstein v. United States Dep't of State, 974 F.Supp. 1288, 1296 (N.D. Cal. 1997). *See infra* notes 68-74 and accompanying text. While printed materials are currently exportable, the government has stated that it reserves the option to impose controls on encryption source or object code in printed form that is scannable. Bureau of Export Administration, *Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List* (visited June 30, 1998) <http://www.bxa.doc.gov/Encryption/encreg.htm>. *See infra* note 68 for an explanation of object and source code. Due to the

As stated earlier, the regulations allow for the exportation of encryption products that would otherwise not be exportable if they contain either a key recovery system or are accompanied by a corporate promise to develop a key recovery system for the product that will support an international key management infrastructure.[21] Recently, however, the Commerce Department has begun to grant licenses to products that do not contain a key recovery system without obtaining a promise from the corporation to develop key recovery.[22] These licenses have been granted because they contain other restrictions upon the export products that the Commerce Department believes will prevent national security and law enforcement interests from being compromised.[23] These restrictions contain such limitations as to which countries and types of business are eligible to obtain the products.

For example, the Commerce Department has been more willing to grant licenses that allow corporations to export products to a few limited countries. Hewlett-Packard was permitted to sell technology that uses 128-bit encryption without including a key recovery system, but only to Britain, Germany, France, Denmark, Australia, and Japan.[24] The Commerce Department has not publicly stated why exceptions were granted only for these countries, but likely reasons are that these countries have encryption controls in place and are close allies of the United States. While these factors do not ensure that the encryption products will be used solely for legal purposes, they do decrease the likelihood that the products will be used for illicit purposes against the United States.[25] However, it is also possible that these exceptions were granted for some other reason. The uncertainty surrounding why these exceptions were granted, and whether similar exceptions will be granted in the future, that makes the application of the regulations by the Commerce Department susceptible to claims of arbitrariness.

Not only are there license exceptions for specific nations, but the Commerce Department has also granted license exceptions to certain corporations for the exportation of encryption to banking and financial insti-

---

First Amendment constitutional issues that the use of this reserved power would raise, it is unlikely that the government will ever attempt to activate this reserved power.

21. 15 C.F.R. §742.15(b)(3) (1998).

22. *See infra* notes 24-31 and accompanying text.

23. *See supra* note 14 and accompanying text.

24. *See, e.g., U.S. Approves HP Encryption Technology Export to Japan*, BUS. DAILY, May 22, 1998, *available in* 1998 WL 12219855.

25. Encryption controls regulate who is using the encryption product and what the product can be used for, while being a close ally decreases the motive for a foreign organization to threaten U.S. national security and law enforcement interests.

tutions. For instance, Cylink, a U.S. company, was permitted to export triple 56-bit encryption to international financial institutions and to subsidiaries of U.S. multinationals without providing for key recovery.[26] This appears to be a concession by the U.S. government to domestic businesses to allow them to compete in a global market. As William A. Reinsch, U.S. Under Secretary of Commerce for Export Administration, stated when the license was announced, "I am pleased we were able to approve the license allowing Cylink to export their strongest encryption products to financial institutions and multinational firms around the world. U.S. companies can and should be able to compete in this rapidly growing market."[27]

On July 7, 1998, the Commerce Department made it easier to sell encryption software to foreign banks by dropping some of the requirements that exporters previously had to satisfy.[28] Under these guidelines, vendors desiring to export encryption only need a one-time product review to sell any bit-length to banks in 45 countries.[29] The products need neither to contain a key recovery system, nor do the exporters have to promise to develop one.[30] Although the July 7 exceptions only applied to financial institutions, the administration's September 16th announcement extends the exception to health-care, medical, and insurance companies.[31]

While the special exceptions allowed have gradually been broadened, they are still the subject of controversy. The exceptions do not satisfy privacy advocates who have criticized that while concessions have been granted to the commercial sector, they have not been extended to individuals.[32] Further, by treating various products, businesses, and countries differently, the exceptions lead to inconsistent and arbitrary outcomes. This becomes apparent when one attempts to create arguments based upon national security and law enforcement that justify why the

---

26. *Cylink*, *supra* note 12. Triple 56-bit is not three times as strong as single 56-bit as one might think, but rather 256 times stronger than single 56-bit. *Id.*

27. *Id.* But see *infra* text accompanying notes 174-176 for other statements by William Reinsch that are not as supportive of looser export controls.

28. *See, e.g., Administration Relaxes Rules on Encryption, A Bit*, 220 N.Y.L.J. S13 (1998) and *Encryption Exporters Win, Lose*, Electronic Messaging News, July 22, 1998, *available in* 1998 WL 7999372.

29. *Id.* The 45 countries are those that comply with international treaties to combat money laundering. *Id.*

30. *Id.*

31. *See White House Statement*, *supra* note 9.

32. *See* Elizabeth Corcoran, *U.S. to Relax Encryption Limits*, WASH. POST, Sept. 17, 1998, at C4, *available in* 1998 WL 16556617; Louise Kehoe, *U.S. and Canada: U.S. Relaxes Encryption Export Curbs*, FIN. TIMES, Sept. 17, 1998, at 8, *available in* 1998 WL 12266245.

businesses that have been granted exceptions have a greater need for privacy than do such businesses as the defense industry or law firms. Nevertheless, the administration intends to continue addressing, on a "case-by-case basis," which end users and nations it should next include within the exception.[33] Unfortunately, these decisions may ultimately have less to do with the foreign policy and security concerns of the United States, and more to do with how effective the exporter is at lobbying. As Bruce Schneier, the President of Counterpane Systems, Inc. put it, "[i]f you have enough money and if you are patient enough, you can get just about anything exported."[34]

B. *What Constitutes An Encryption Export*

Now that the current encryption export policies have been set forth, it is necessary to examine what exactly constitutes an exportation of encryption. The EAR defines an export as "an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States."[35] But the regulations on encryption have an additional definition for the exportation of encryption source code and object code. This definition states that for the purposes of the encryption software regulations the word "exporting" includes the

> [D]ownloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., *or* making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo-optical, photoelectric or other comparable communications facilities *ac-*

---

33. *See White House Statement, supra* note 9.

34. Jim Kerstetter, *Crypto Holes Slow Export Adoption: Arbitrary Rulings Confuse ISV's, Users*, PC WEEK, June 1, 1998, at 8. Lobbying efforts on behalf of encryption exports have increased dramatically in recent years and a large reason for this has been the formation and success of the lobbying group Americans for Computer Privacy (ACP). Andrew Mollison, *Coalition Near Compromise on Encryption Laws: By Creating Lobbying Army, Group on Cusp of Deal With Security Agencies to Allow Export of Codes*, ATLANTA J. & ATLANTA CONST., Aug. 1, 1998, at A8, *available in* 1998 WL 3707039. The ACP was formed in 1997 after Congress was unable to pass legislation allowing greater encryption exports. *Id.* Since its inception the ACP has grown to include more than 40 associations, 90 companies, and 2000 individuals and as of August 1997 had the authority to spend between five and eight million dollars. *Id.* This is in addition to the more than seven million dollars that its members have contributed in federal campaign contributions in the course of a year and a half. *Id.*

35. 15 C.F.R. §734.2(b)(1) (1998).

> *cessible to* persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites.[36]

Although this definition appears to be very comprehensive when combined with the traditional definition, it is not foolproof. For example, as stated earlier a printed book containing encryption source code is not subject to the EAR and therefore can be exported.[37] Once such a book is obtained anyone using a scanner or anyone able to type will be able to input this material into a computer and transform it into object code. Even though the U.S. government has stated that it has reserved the right to impose controls on encryption source code in printed form that is scannable, such exports are currently permitted.[38] This makes the EAR distinction between source code in printed form which is exportable and source code in electronic form which requires a license ineffective because the license requirement can easily be circumvented.

Not only do the definitions contain loopholes, but they also cover some actions that arguably should not be considered as constituting an export. For example, while the mere posting of a program to a file transfer protocol (FTP) or web server located in the United States constitutes an export according to the definition, the mere posting of such a program does not by itself result in any sending, taking, disclosure or transmission of the program to a foreign person.[39] Though the definition classifies the mere posting of encryption as an export, it does include a caveat that permits encryption products to be placed on Internet sites within the United States as long as the provider implements safeguards that are "adequate to prevent unauthorized transfer of such code outside the United States."[40] The required precautions include making sure that access to and transfer of the software is controlled through such measures as: (1) checking the address of every system attempting to obtain the software to make sure that the system is located within the United States; (2) providing a requesting party with notice that the transfer of the software is subject to export controls and that it cannot be exported without a license; and (3) requiring every party requesting a transfer to acknowledge that they understand that the software is subject to export controls.[41]

---

36. 15 C.F.R. §734.2(b)(9)(ii) (1998) (italics added).
37. 15 C.F.R. §734.3(b)(2) (1998). *See supra* text accompanying notes 19-20.
38. *See supra* note 20.
39. *See* Rubinstein, *supra* note 3, at 342.
40. 15 C.F.R. §734.2(b)(9)(ii) (1998).
41. 15 C.F.R. §734.2(b)(9)(ii)(A)(1-3) (1998).

However, since it is nearly impossible for most Internet users to satisfy these precautions, ultimately almost any posting of software on the Internet will be an export.[42] Even if satisfied, these precautions are not full-proof because they still do not ensure that the regulated encryption will stay only within the hands of U.S. citizens as the regulations require. A foreign person who has signed up for Internet access using a U.S. Internet Service Provider (ISP) and who signed into the secure download site either from within the United States or who payed long distances charges to dial-in to a U.S. ISP from an overseas location, would be granted access to the encryption information.[43] Even if a vendor follows the guidelines, there is no guarantee that the vendor will be shielded from liability in the event that a controlled item is exported.[44]

In addition to containing loopholes and being circumvented, the exportation regulations can be confusing and unclear. The export controls on encryption software were once so broad that many business executives who traveled overseas with their laptop computers undoubtedly violated the controls since many standard off-the-shelf office and business programs were subject to the export regulations.[45] The EAR have since been clarified to permit the temporary export of encryption hardware and software, but the regulations continue to require that the temporary exporter retain control of the computer throughout the trip, that the computer be for the temporary exporter's exclusive and personal use and that it not be used for copying, demonstration, marketing, or sale.[46] If the temporary export is not for the exporters personal use, then different, more stringent regulations apply in addition to those required for personal use.[47] There are also detailed controls on the use of the programs for demonstrations and exhibitions,[48] the destinations to which the en-

---

42. *See* Junger v. Daley, 8 F.Supp.2d 708 (N.D. Ohio 1998) (acknowledging that it is "nearly impossible for most Internet users to carry out or verify these precautions.")

43. *See* RUBINSTEIN, *supra* note 3, at 344.

44. *See id.* It is more likely that the vendor's web site would be shut down than that he or she would be prosecuted. *Id.*

45. *See* MIDDLEHURST, ET AL., *supra* note 6, at 554.

46. 15 C.F.R. §740.9(a) (1998).

47. 15 C.F.R. §740.9(a)(2)(iii) (1998).

48. *Id.* For example, the regulations on exhibitions and demonstrations require that the exporter: (1) retain ownership of the software or commodity; (2) retain effective control of the product; (3) not use the product for its intended purpose while abroad, except to the minimum extent required for effective demonstration; and (4) not demonstrate or exhibit the product at any one site for more than 120 days. 15 C.F.R. §740.9(a)(2)(iii) (1998). In addition, no commodity or software may be exported if an order to acquire the product has been received before shipment. 15 C.F.R. §740.9(a)(3)(iii)(A) (1998). What this means is that once an order to acquire a commodity or software has been received, the product cannot be exported for exhibition or demonstration purposes even if the dem-

cryption commodity or software can be exported,[49] the length of time that a product can be exhibited or demonstrated,[50] rules on when an exporter will be authorized to retain the product abroad for more than a year,[51] and restrictions on the permanent export or re-export of products that are temporarily abroad,[52] all of which can create substantial confusion and uncertainty among businesses and lawyers alike as to the proper course of action for any given product.

C. *Circumvention Of The Encryption Regulations*

One of the things that threatens to undermine the government's ability to regulate encryption is that it is virtually impossible to guarantee the success of future controls, because all controls are susceptible to circumvention. Not only are there ways for foreigners to circumvent U.S. controls and obtain encryption information,[53] but the controls are also being avoided by U.S. persons and industries. A few U.S. businesses are attempting to do this by setting up subsidiaries in foreign countries to license encryption products made by foreign companies and sell them to overseas markets.[54] This is legal as long as the U.S. parent company does not provide any technical assistance to the subsidiary and distributes the products from distributors outside the United States.[55] Currently several

---

onstration or exhibition were to occur in a different country from where the order originated. In other words, once an order to acquire has been received, the product cannot be exported anywhere without a license.

49. 15 C.F.R. §740.9(a)(3)(i) (1998).

50. 15 C.F.R. §740.9(a)(2)(iii) (1998).

51. 15 C.F.R. §740.9(a)(4)(iii) (1998).

52. 15 C.F.R. §740.9(a)(4)(i) (1998).

53. *See supra* note 43 and accompanying text. In addition to those previously mentioned, circumvention also occurs when foreign companies purchase American- produced 56-bit encryption technology and then upgrade it in their own countries to 128-bit technology. Rep. Adam Smith, *Encryption Laws Stymie U.S. Competitiveness*, PUGET SOUND BUS. J., Sep. 19, 1997, at 63 *available in* 1997 WL 11543883. This was done recently by a group of Australian software developers who obtained from Netscape the source code for the web browser Netscape Communicator that has a 40-bit encryption capability and within 15 hours had built a generic browser that contained 128-bit capabilities. Stan Beer, *Secure Code Slips US Net*, AUSTL. FIN. REV., Apr. 7, 1998, at 41, *available in* 1998 WL 9425566.

54. *See infra* note 56.

55. Greg Miller, *Network Associates Crafts Overseas Deal to Sell Encryption Trade: Its Subsidiary Would License Product from Swiss Firm to Avoid Restrictions*, L.A. TIMES, Mar. 20, 1998, at D1, *available in* 1998 WL 2409888. As stated earlier the U.S. export restrictions only forbid the shipment of actual software while permitting the publication of written source code. *Id. See also supra* text accompanying note 19-20.

companies plan to create such arrangements.[56]

The U.S. regulatory agencies have expressed concern over this developing situation which stems from the fact that the businesses are following "the letter, if not the spirit" of the law.[57] In an attempt to curtail this development, the Commerce Department closely scrutinized those companies which announced plans to create such arrangements and has threatened investigations.[58] Although as of yet the Commerce Department has not taken any action against such companies, the close scrutiny has probably prevented this circumvention technique from becoming widespread.[59] But if the arrangements that are currently being set up by U.S. companies are able to avoid penalties from the Commerce Department, then undoubtedly the number of such arrangements will increase quickly. This would force the U.S. government into a precarious situation because there is very little that it would be able to do against the foreign subsidiaries selling the products and even less that it would be able to do against the foreign corporations that are creating the encryption.

III. RELEVANT CASE LAW

Circumvention, confusion, and arbitrariness are not the only problems surrounding the regulation of encryption exports. Three principal cases exist involving challenges to the government's encryption export regulations.[60] In *Karn v. United States Department of State*,[61] the

---

56. Sun Microsystems planned to market Russian-made encryption software to foreign customers from distributors outside the United States. Don Clark, *Sun Is Holding Off on Plans to Market Russian-Made Encryption Software*, WALL ST. J., Mar. 9, 1998, at B8, *available in* 1998 WL 3485421. However, Sun Microsystems has not yet marketed the product because it is a major computer supplier to the U.S. government and felt an obligation to be a "good citizen" and therefore decided to respect the Commerce Department's concerns. *Id.* Network Associates, Inc. is another example of circumvention by a U.S. business. A Swiss company has developed a product that uses source code published by Network Associates. Miller, *supra* note 55, at D1. A European subsidiary of Network Associates has licensed the product and is planning to sell it in overseas markets. *Id.* Entrust is a final example of this type of circumvention. Entrust is a Canadian company that has an American parent company named Nortel. Entrust sells a 128-bit encryption program for less than $50. Smith, *supra* note 53, at 63.

57. Miller, *supra* note 55. William Reinsch, Under Secretary of Commerce, has acknowledged that if Network Associates only provides published source code, the company would not be in technical violation of the regulations. *Id.*

58. *Id.*

59. *Id.*

60. However, the dispute that has been most widely covered which involved Phillip Zimmerman and his encryption program Pretty Good Privacy (PGP), did not spawn legal proceedings. *See* MIDDLEHURST, ET AL., *supra* note 6, at 554. Although the government did investigate Zimmerman for export violations, he was never prosecuted and the

U.S. District Court for the District of Columbia held that even if source code constituted speech for First Amendment purposes, Karn's free speech rights were not violated because U.S. foreign policy and national security concerns provided sufficient reasons to uphold the regulations.[62] *Junger v. Daley*[63] is another case that has upheld the government regulations. In *Junger*, a U.S. District Court in Ohio ruled that the regulations are constitutional because encryption source code is inherently functional, the regulations are not directed at the expressive elements of source code, and the regulations do not reach academic discussions of software or software in print form.[64] There has not however, been a universal consensus among the courts as to the constitutionality of the current regulations. There has in fact been one case that has held that the current encryption export regulations are unconstitutional. In *Bernstein v. United States Department of State*,[65] a U.S. District Court in California concluded that the encryption regulations are an unconstitutional prior restraint on expression that is protected by the First Amendment.[66]

How these contradicting interpretations of the First Amendment are ultimately resolved by the appellate courts will affect the encryption regulations and influence the form and scope of future regulations. If the reasoning in *Karn* and *Junger* is upheld, then the current regulations could continue indefinitely and any similar future regulations would be likely to withstand First Amendment challenges. But if the reasoning used in the *Bernstein* case eventually prevails, then the current regulations as well as any future regulations will have to be drafted more conscientiously to avoid potential First Amendment pitfalls that would undermine their validity. It is therefore necessary to evaluate all three of the cases and understand the reasoning behind them in order to determine how their eventual resolution might affect future government regulations.

A. *The Bernstein* Case

Daniel Bernstein, while a graduate student at the University of California at Berkeley, developed an encryption algorithm called "Snuffle."[67] Bernstein expressed his algorithm as an academic paper entitled "The Snuffle Encryption System" and also as source code that was written in

---

charges were eventually dropped. *Id.*

61. 925 F.Supp. 1 (D.D.C. 1996).
62. *Karn*, 925 F.Supp. at 1, 9.
63. No. 1:96-CV-1723, 1998 WL 388972 (N.D. Ohio).
64. *Junger*, 1998 WL 388972, at *1.
65. 974 F.Supp. 1288 (N.D. Cal. 1997).
66. *Bernstein*, 974 F.Supp. at 1308.
67. *Id.* at 1293.

"C."[68] Bernstein then submitted a commodity jurisdiction request to the Office of Defense Trade Controls (ODTC) to determine whether the paper and the source code were controlled by the International Traffic in Arms Regulations (ITAR).[69] In response, the ODTC, after consultations with the Departments of Commerce and Defense, determined that Snuffle was a defense article and was subject to licensing requirements prior to export.[70] Bernstein subsequently submitted a second request in July of 1993 to determine whether the academic paper had been included as part of the prior ODTC decision.[71] The ODTC informed Bernstein that the paper was indeed a defense article and that it required a license.[72] However, after Bernstein initiated legal proceedings the ODTC clarified in a letter that the paper was actually not a defense article.[73] Nevertheless, the ODTC still maintained that the electronic versions of Snuffle, as well as the explanations and descriptions of how to use and program Snuffle onto a computer, were defense articles subject to ODTC control.[74] The ODTC's position led Bernstein to bring an action that challenged the classification of the electronic version of Snuffle as a defense article.[75] Bernstein claimed that the laws upon which the classification were based, the Arms Export Control Act (AECA)[76] and the ITAR, were both unconstitutional on their face and as they applied to him, because they violated the First Amendment by preventing him from teaching, publishing or dis-

---

68. *Id.* Bernstein's program in "C" language detailed both the encryption and the decryption procedures of Snuffle. *Id.* "C" is a high-level computer programming language. *Id.* (footnote omitted). Once source code such as "C" is converted into object code by a computer, it is possible for the computer to encrypt and decrypt data. *Id.* Object code is a binary system that consists of a series of 0's and 1's. *Id.*

69. 22 C.F.R. §§120-30 (1994). Bernstein v. United Stated Dep't of State, 922 F.Supp. 1426, 1430 (N.D. Cal. 1996). Before Executive Order 13026 was issued on November 15, 1996 the ODTC, rather than the EAA, had jurisdiction over the exportation of encryption. *Bernstein*, 974 F.Supp. at 1293. *See infra* notes 85-87 and accompanying text.

70. *Bernstein*, 922 F.Supp. at 1430.

71. Bernstein v. United States Dep't of State, 945 F.Supp. 1279, 1284 (N.D. Cal. 1996). It is probable that Bernstein submitted a second request because the ODTC had identified Snuffle within the first request as a "stand-alone cryptographic algorithm which is not incorporated into a finished software product." *Id.* The ODTC had also informed Bernstein that "a commercial software product which incorporated Snuffle might not be subject to State Department control and should be submitted as a new request." *Id.*

72. *Id.* at 1285.

73. *Id.*

74. *Id.*

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

76. 22 U.S.C.A. §2778 (1994).

cussing with other scientists his theories on cryptography.[77]

In the first action between Bernstein and the United States Department of State (*Bernstein I*),[78] the District Court held that the "C" source code was speech for purposes of the First Amendment and that Bernstein's claims were therefore justiciable.[79] One argument propounded by the government was that the encrypting of electronic communications served a functional purpose rather than a communicative one.[80] Therefore, according to the government, the program was not speech but rather conduct which should only be protected if it is "sufficiently imbued with the elements of communication."[81] Judge Patel rejected this argument, concluding that "the functionality of a language does not make it any less like speech" and that the communicative nature of conduct need be inquired into only after determining that the act at issue is indeed conduct rather than speech.[82]

In the second action between these two parties (*Bernstein II*),[83] the same court concluded that the licensing requirements applicable to encryption software under the ITAR constituted an unlawful prior restraint to the First Amendment.[84] However, before the court issued its order, President Clinton issued Executive Order 13026, which transferred jurisdiction over the export of nonmilitary encryption products to the Department of Commerce pursuant to the Export Administration Act of 1979[85]

---

77. *Bernstein*, 974 F.Supp. at 1293.

78. 945 F.Supp. 1279 (N.D. Cal. 1996).

79. *Bernstein*, 974 F.Supp. at 1293. The court stated that it could find "no meaningful difference between computer language, particularly high-level languages as defined above, and German or French." Bernstein v. United States Dep't of State, 922 F.Supp 1426, 1435 (N.D. Cal. 1996). *But see* John P. Collins, Jr., Note, *Speaking in Code*, 106 YALE L.J. 2691 (1997) (concluding that cryptographic computer source code is conduct not entitled to protection by the First Amendment and that the court in *Bernstein* was incorrect in categorizing it as speech). See also Thinh Nguyen, Note, *Cryptography, Export Controls, and the First Amendment in Bernstein v. United States Department of State*, 10 HARV. J.L. & TECH. 667 (1997), for an analysis of the decision to include source code as speech that is protected by the First Amendment.

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

81. *Id.* at 1434 (citing Texas v. Johnson, 491 U.S. 397, 404 (1989)). *See also* Spence v. Washington, 418 U.S. 405, 409 (1974) (per curiam).

82. *Bernstein*, 922 F.Supp. at 1435. The *Bernstein* court believed that *Johnson* and *Spence* imply that a court need only assess the expressiveness of conduct in the absence of "the spoken or written word'" which meant that it was not applicable in the instant case because the encryption system was written. *Id.* at 1434-35 (citing *Johnson*, 491 U.S. at 404).

83. 922 F.Supp. 1426 (N.D. Cal. 1996).

84. *Bernstein*, 974 F.Supp. at 1293. In this decision the court also looked at "vagueness and ovér breadth challenges to certain terms contained in the ITAR." *Id.*

85. Export Administration Act of 1979, 50 App. U.S.C.A. §§2401-2420 (1998).

(EAA) and the Export Administration Regulations (EAR) while encryption for military purposes would continue to be regulated by the ITAR.[86] Using its newfound authority, the Commerce Department issued new rules regulating the export of certain encryption products.[87] These new regulations permitted some additional exceptions for certain commercial encryption items, including exportation of software without key recovery of up to 56-bit key length as long as the manufacturer made a commitment to develop a key recovery system.[88]

Bernstein subsequently amended his complaint to include the new regulations and new defendants.[89] The issue before the court in the latest action was whether the amendments to the EAR mandating licensing requirements for the export of cryptographic devices, software and related technology, constituted a prior restraint on speech in violation of the First Amendment.[90] Because the regulations that control the exportation of encryption are no longer currently under the ITAR, the court first had to determine whether the transfer of jurisdiction to the Commerce Department was valid.[91] Once satisfied that the transfer was valid, the court turned its attention to deciding whether the Commerce Department had created regulations that constituted a prior restraint to free speech while failing to provide the necessary safeguards.[92]

---

86. *Bernstein*, 974 F.Supp. at 1293.

87. Encryption Regulations, 61 Fed. Reg. 68,572 (1996) (codified at 15 C.F.R. Pts. 730-774).

88. *See, e.g.*, Richard R. Mainland, *Congress Holds the Key to Encryption Regulation*, 20 NAT'L L.J. 34, B9 (1998). Remember that this has again changed so that encryption with key lengths of 56-bits or less can now be exported without key recovery. *See supra* text accompanying notes 12-16,

89. *Bernstein*, 974 F.Supp. at 1292. The new defendants included the Department of Energy, the Department of Justice, and the Central Intelligence Agency. *Id.* at 1309.

90. *Id.* at 1292.

91. *Id.* at 1297. The court states that the International Emergency Economic Powers Act (IEEPA) is broad enough to encompass encryption and that therefore the President can regulate encryption under the IEEPA because encryption does not come within one of the exceptions to the IEEPA. *Id.* at 1297. The court did not review whether the President exceeded his authority when he transferred jurisdiction, because he acted under the authorization of Congress thus giving the transfer the strongest presumption of validity. *Id.* at 1297, 1300. The court also decided that the Department of Commerce had the proper authority to regulate encryption under the IEEPA. *Id.* at 1300. Finally, the court found that encryption does come within the meaning of the regulation, that communications dealing with encryption have value and that encryption products do not fall within the exemption for informational materials provided by the statute. *Id.* at 1301-02. Therefore, according to the court although the government has "the authority to regulate encryption source code, they must nonetheless do so within the bounds of the First Amendment." *Id.* at 1303.

92. *Id.* at 1300.

As the Supreme Court has stated and as the court in *Bernstein* pointed out, "it has been generally, if not universally, considered that it is the chief purpose of the [First Amendment] guaranty to prevent previous restraints upon publication."[93] Thus, any prior restraint on the First Amendment has a "heavy presumption" against its constitutional validity.[94] Nevertheless, the government can impose valid time, place and manner restrictions when they are content neutral, narrowly tailored to serve a substantial interest, and leave open alternative channels for communication.[95] However, such valid content neutral restrictions on expression may not be conditioned upon obtaining a license from a government official when that official has "boundless discretion."[96] In addition, the *Bernstein* court stated that an item does not have to be regulated for its content in order for the regulations to function as a prior restraint since the regulation of expressive activity is also sufficient to create a prior restraint under the Supreme Court plurality opinion of *FW/PBS, Inc. v. City of Dallas*.[97]

Consequently, because the *Bernstein* court had already determined in its previous decisions that source code constituted expressive activity, the court used the *Freedman* test to examine whether the Commerce Department had established procedural safeguards that would validate the prior restraint created by the licensing scheme.[98] The *Freedman* test states that for a licensing scheme to be constitutional, "1) the licensor must make the licensing decision within a specific and reasonable period of time; 2) there must be prompt judicial review; and 3) the censor must bear the burden of going to court to uphold a licensing denial and once there bears the burden of justifying the denial."[99]

The court in *Bernstein* found that the current EAR procedures lack any standards for deciding an application and impose no limits on agency discretion, stating that the constraints were "illusory" and that it allows

---

93. *Id.* at 1303 (citing Near v. Minnesota, 283 U.S. 697, 713 (1931)).

94. Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971) (citations omitted).

95. Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984).

96. Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 764 (1988).

97. *Bernstein*, 974 F.Supp. at 1307 (citing FW/PBS, Inc. v. City of Dallas, 493 U.S. 215, 223 (1990) (plurality opinion)). In FW/PBS, the plurality opinion stated that "[B]ecause we conclude that the city's licensing scheme lacks adequate procedural safeguards, we do not reach the issue decided by the Court of Appeals whether the ordinance is properly viewed as a content-neutral time, place, and manner restriction aimed at secondary effects arising out of the sexually orientated businesses." *FW/PBS*, 493 U.S. at 223 (plurality opinion).

98. *Bernstein*, 974 F.Supp. at 1307-08.

99. *FW/PBS*, 493 U.S. at 227-28 (plurality opinion).

the BXA to deny an application by claiming that it is "contrary to national security and foreign policy interests" without having to provide any additional reasons.[100] Therefore, the court concluded that the licensing scheme was "woefully inadequate" and an unconstitutional prior restraint in violation of the First Amendment without providing the necessary safeguards.[101]

The court also analyzed whether the government's national security and foreign policy rationales justified the prior restraints. The court used language from *New York Times Co. v. United States*,[102] that stated that national security and foreign policy by themselves are not sufficient to justify a prior restraint such as a licensing scheme.[103] Therefore, the *Bernstein* court found that because national security and foreign policy reasons were the only justifications provided by the government, regulations that constitute a prior restraint cannot be upheld on those grounds,[104] particularly when, according to the court, "none of the encryption items subject to export controls under the EAR have military applications."[105]

B. *The Karn Case*

In 1994 Phil Karn, a computer engineer, submitted a commodity jurisdiction request to the Department of State for a book containing encryption algorithms.[106] In response to this request, the Department of State's Office of Defense Trade Controls (ODTC) determined that the

---

100. *Bernstein*, 974 F.Supp. at 1308. The court was also concerned with the fact that although license applications must be resolved or referred to the President within 90 days, there is no time limit on an application that has been referred to the President. *Id.* In addition, if a license is denied, there is not a definite time limit on the appeals decision and that decision is not subject to judicial review. *Id.*

101. *Id.* In addition, even though the court had already determined from the prior proceedings that the encryption material was speech, the court pointed out that the distinction between print and electronic media was untenable and that the Internet was subject to the same exacting level of First Amendment scrutiny as print media. *Id.* at 1306-07.

102. 403 U.S. 714 (1971).

103. *Bernstein*, 974 F.Supp. at 1307. The court also stated that although prior restraints could be overridden in times of war, even then they would be limited to when disclosure would "surely result in direct, immediate, and irreparable damage to our Nation or its people." *Id.* at 1307, quoting *New York Times Co.*, 403 U.S. at 730.

104. *Bernstein*, 974 F.Supp. at 1307.

105. *Id. See supra* text accompanying notes 85-86.

106. Karn v. United States Dep't of State, 925 F.Supp. 1, 3 (D.D.C. 1996). The book contained source code for several powerful encryption algorithms that were written in the "C" programming language. RUBINSTEIN, *supra* note 3, at 338. *See* discussion *supra* note 68.

book was not subject to the jurisdiction of the International Traffic in Arms Regulations (ITAR) since the item was in the "public domain."[107] The ODTC explained that the ruling only covered the book and not the source code disks available from the author even though they both contained the same materials, because the diskette was designated as a "defense article" under the United States Munitions List and therefore subject to additional regulations.[108] The ODTC justified this position by stating that the text files on the disk were not identical to the source code printed in the book, since "[e]ach source code listing has been partitioned into its own file and has the capability of being easily compiled into an executable subroutine."[109]

Unhappy with this result, Karn filed a federal lawsuit that raised First and Fifth Amendment claims and also alleged that the commodity jurisdiction denial was an abuse of administrative discretion under the Administrative Procedure Act (APA).[110] The APA claim was dismissed by Judge Richey as non justiciable.[111] Richey stressed that this case was a "political question" for the two elected branches and that it presented a "classic example" of how courts can be needlessly invoked in litigation over foreign policy issues because the plaintiff has not been able to persuade the elected branches that the technology at issue does not endanger national security.[112] Richey went on to find that the commodity jurisdiction procedure used for the Arms Export Control Act (AECA) and the ITAR as well as the designation of the diskette as a "defense article" were not subject to judicial review.[113]

---

107. RUBINSTEIN, *supra* note 3, at 338. Although the decision in *Karn* was based upon the AODTC" and the ITAR rather than the EAA and the EAR, it is still useful as a forecaster of how this court will approach the First Amendment issue in future cases.

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

109. RUBINSTEIN, *supra* note 3, at 338.

110. *Karn*, 925 F.Supp. at 3.

111. *Id.* However, the United States Court of Appeals for the District of Columbia Circuit remanded the case to the District Court to determine "the reviewability of and, if appropriate, the merits of appellant's claim under the Administrative Procedure Act." Karn v. United States Dep't of State, 107 F.3d. 923, 1 (D.C. Cir. 1997). The remand was the result of the transfer of regulatory authority to the Commerce Department and the new regulations which were subsequently promulgated. *Id.* The Court of Appeals stated that courts should always first consider alternative grounds for resolution whenever they are asked to answer a question involving the Constitution. *Id.* Regardless of the remand, the *Karn* case is still useful as a guide as to how courts in future cases may decide to resolve the First Amendment issue, especially since the court in *Bernstein* determined that the APA does not create any justiciable claims. Bernstein v. United States Dep't of State, 974 F.Supp. 1288, 1298 (N.D. Cal. 1997).

112. *Id.*

113. *Karn*, 925 F.Supp. at 5-6. Richey interpreted Section 2778(h) of the AECA as

Karn also did not prevail on his constitutional claims. The court stated that even though constitutional challenges would normally be allowable for the disputed regulations, they were not justified here because there were no material facts in dispute regarding the First Amendment since the regulation was content neutral and satisfied an intermediate level of scrutiny as established by the *O'Brien* test.[114] The *O'Brien* test states that content neutral regulations may be justified if the regulation is (1) within the constitutional power of the government, (2) "furthers an important or substantial governmental interest," and (3) is narrowly tailored to the governmental interest.[115] According to the court, the three requirements of the *O'Brien* test were all satisfied in *Karn*, the first two being undisputed by the plaintiff, and the third because the plaintiff did not present a satisfactory argument as to why the regulation was not narrowly tailored.[116] The court wrote that the President's decision to restrict the export of encryption software by placing it on the ITAR was a foreign policy decision that could not be scrutinized, even though the encryption was already available overseas which would seem to prevent the current regulations from furthering U.S. national security.[117] Also of significance are the court's statements that the plaintiff did not have standing to argue the claim that certain provisions of the ITAR constituted an unconstitutional prior restraint, since the provisions had not yet been applied to the plaintiff.[118] The *Karn* court was therefore able to avoid the

---

precluding judicial review over not only the act of listing items on the munitions list which is what the plaintiff desired, but also as precluding the determination of whether things such as the diskette was actually covered by an item on the munitions list. *Id.* Although the court conceded that normally judicial review is allowed absent clear and convincing evidence of legislative intent to preclude it, the court concluded that in the current situation that the legislature had intended for judicial review to be precluded. *Id.* at 6.

114. *Id.* at 9-11. The regulation is content neutral according to the court, because the government is not regulating the "expressive content of the comments and or source code, but instead [is] regulating because of the belief that the combination of encryption source code on machine readable media will make it easier for foreign intelligence sources to encode their communications." *Id.* at 10. The court in *Karn* also concluded that it was unnecessary to determine the nature of the materials contained on the diskette, because the government rationale behind the regulation was the controlling factor and that the form of the speech or expression regulated was not important. *Id.* Nor did it matter to the court that the book form of the encryption was treated differently than the diskette form. *Id.*

115. United States v. O'Brien, 391 U.S. 367, 388 (1968).

116. *Karn*, 925 F.Supp. at 10-11.

117. *Id.* at 11. The court recognized that the plaintiff's argument as to the third requirement actually concerned the second requirement and dealt with it accordingly. *Id.*

118. *Id.* at 12.

prior restraint argument that was used by the *Bernstein* court to find in favor of the plaintiff.

C. *The Junger Case*

Peter Junger is a law professor who maintains sites on the World Wide Web that contain information about the courses that he teaches, including a course on computers and the law.[119] Junger wanted to post to his web site various encryption programs that he had written to show how computers work.[120] However, as discussed earlier such postings are a violation of the export regulations.[121] Junger therefore submitted applications to the Commerce Department requesting a determination of the commodity classifications for the encryption software programs.[122] The Commerce Department informed Junger that the software was covered by the regulations and required an export license.[123]

Junger filed suit claiming that the licensing requirements for the exportation of encryption software constitute a prior restraint that violate the First Amendment's free speech clause.[124] Although the court conceded that encryption source code may occasionally be expressive, it found that its export was still not protected conduct under the First Amendment.[125] The court came to this conclusion by determining that encryption software is functional rather than expressive and that it is rarely used to communicate ideas.[126] As such, encryption source code according to the court is exported to transfer functions, not to communicate ideas

---

119. *Junger*, 8 F.Supp.2d at 713-14 (N.D. Ohio 1998).

120. *Id.*

121. *See supra* text accompanying notes 39-44.

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

123. *Id.*

124. *Id.* at 711. Junger also had four other counts within his complaint that the court ruled upon. *Id.* At 711-12. In Count Two the court found that the regulations were not over broad because they do not injure third parties in a different manner from the way they affected Junger and that the regulations are not vague. *Id.* With regard to Count Three, the court found that even though the regulations subject encryption to more stringent restrictions than other items, that the regulations are content neutral and able to pass an intermediate level of scrutiny because they allow the government to collect vital foreign intelligence, are not directed at a source code's idea, and do not burden more speech than is necessary. *Id. See supra* notes 114-15 and accompanying text for the intermediate level of scrutiny as established by *O'Brien*. The court found that Count Four had been waived by Junger. *Id.* As for Count Five, the court found that it did not have the jurisdiction to review whether the President exceeded his authority under the IEEPA when he directed that encryption products be controlled for export. *Id.*

125. *Id.* at 712. *See supra* note 80-82 and accompanying text to compare how this functionality argument was treated by the *Bernstein* court.

126. *Id.* at 715-18.

and that the value to the importer stems from the function that the source code performs.[127] Because the court acknowledged that the exportation of source code could occasionally be expressive, it went through the guidelines provided by the Supreme Court that establish when occasionally expressive conduct is "sufficiently imbued with the elements of communication to fall within the scope of the First . . . Amendment."[128] As stated by the Supreme Court, to be protected by the First Amendment "an intent to convey a particularized message [must be] present, and in the surrounding circumstances the likelihood [must be] great that the message would be understood by those who viewed it."[129] The *Junger* court in applying this standard stated that encryption source code did not convey "an unmistakable message" and that the communicative nature of source code is not "overwhelmingly apparent" and therefore found that the export of source code software was not protected conduct under the First Amendment.[130]

Similarly the court found that "the prior restraint doctrine is not implicated simply because an activity may on occasion be expressive."[131] The court justified its decision by comparing encryption to a case from the Ninth Circuit which held that an anti-sitting ordinance that impaired the expressive acts of sitting or lying on the sidewalk was not an unconstitutional prior restraint because such actions are not "integral to, or commonly associated with, expression."[132] The court also stated that for a licensing law to be invalidated by a prior restraint challenge, it "must have a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat" of censorship.[133] The court concluded that encryption source code was not "integral" to expression and has little expressive nature because source code is normally only a set of instructions to a computer that is used to control its operation.[134] After coming to these conclusions, the court granted

---

127. *Id.*

128. *Junger*, 8 F.Supp.2d at 717 (citing Spence v. State of Washington, 418 U.S. 405, 409-10 (1974) (per curiam)). This is the same test that the *Bernstein* court analyzed. *See supra* notes 80-82 and accompanying text.

129. *Id.* (citing *Spence*, 418 U.S. at 411).

130. *Id.* (citing Texas v. Johnson, 491 U.S. 397, 406 (1989) and Tinker v. Des Moines Independent Community School Dist., 393 U.S. 503, 505-06 (1969)).

131. *Id.* at 717-18.

132. *Id.* at 718 (citing Roulette v. City of Seattle, 97 F.3d 300, 304 (9th Cir.1996)).

133. *Id.* at 718 (citing City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 759 (1988)).

134. *Junger*, 8 F.Supp.2d at 718.

summary judgment for the U.S. government on the First Amendment arguments set forth by Junger.[135]

D. *Comparing Bernstein, Karn, and Junger*

The most interesting aspect of the three cases is that they were decided so differently even though they arose from similar facts. Despite their contradictory outcomes, the cases do agree in some areas. They all agree that books, academic writings, and papers can be exported without a government license, because they are "protected speech" under the First Amendment.[136] The *Karn* and *Bernstein* courts, the two courts that examined the issue, also agreed that although the AECA and the EAA/EAR bar judicial review of the designation of encryption items as defense items, they do not bar constitutional claims regarding the regulations themselves.[137]

But while the courts agreed on these points, they disagreed on several other issues. Although the electronic forms of the encryption were the source of controversy in both cases, *Bernstein* stressed the glaring inconsistency of allowing some forms of export but not others[138] while *Karn* determined that this was a valid distinction.[139] More importantly, the courts disagreed over whether the government regulations constituted valid restrictions upon the plaintiffs' First Amendment rights and whether the exports of encryption were expressive or functional.[140] The *Karn* court found that the ITAR regulations were content neutral and justifiable restrictions under the *O'Brien* test and that it did not have to decide whether the regulations constituted a prior restraint on the First Amendment.[141] Likewise, the *Junger* court found that encryption exports were only occasionally expressive and therefore not protected by the First Amendment and also that the regulations themselves were content neutral and satisfied the *O'Brien* test.[142] The *Bernstein* court however, decided that even if the regulations were content neutral, the encryption system was pure speech that could not be limited by a prior restraint without establishing sufficient safeguards.[143]

---

135. *Id.* at 711.

136. *See, e.g.*, RUBINSTEIN, *supra* note 3, at 340.

137. *Id.*

138. Bernstein v. United States Dep't of State, 974 F.Supp. 1288, 1306 (N.D. Cal. 1997).

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

140. *See, e.g.*, RUBINSTEIN, *supra* note 3, at 339.

141. *See supra* text accompanying notes 114-118.

142. *See supra* notes 124-126 and accompanying text.

143. *See supra* text accompanying notes 83-85 and 98-100.

Although the reasoning used by the court in the *Karn* case is persuasive on many points, the court side-stepped both a decision as to whether the regulations actually further the government's national security interest and a prior restraint analysis, the latter being an issue that later proved to be decisive in the *Bernstein* cases. The *Junger* court also concluded that the prior restraint doctrine was not at issue, because the exportation of encryption software was inherently functional and only occasionally expressive.[144] In coming to its conclusion the court in *Junger* while acknowledging the argument that a court need only assess the expressiveness of conduct in the absence of "the spoken or written word," emphasized that "what determines whether the First Amendment protects something is whether it expresses ideas."[145] The court went on to detail how "fighting words" are excluded from First Amendment protection and how commercial advertisements are held to a lesser level of protection, but then failed to explain why these arguments were applicable to encryption, choosing instead to focus on encryption's functionality.[146]

Moreover, the court does not mention all of the ways that encryption can be expressive. In other words, by focusing on the fact that encryption source code is often exported to transfer encryption functions, the court overlooks the fact that source code is often the "natural" and "best" means of communication for some types of ideas such as mathematical algorithms.[147] The court also overlooks the possibility that this transfer of functions is itself expressive. The transfer expresses the idea that people should have the right to converse in private and be able to exclude other people from their private conversations. A licensing law that prevents the transfer may therefore constitute a real and substantial threat of censorship because the law may result in those conversations not taking place. Given this line of reasoning, in addition to those outlined by the cases themselves, it is the prior restraint doctrine as applied in *Bernstein,* rather than in *Junger*, which is the more convincing and the one that should be applied by the appellate courts. However, given the wide range of beliefs concerning this issue, this conclusion is far from certain.

Not only do the three decisions have conflicting results as to the constitutionality of the current regulations, they also leave unresolved many of the inconsistencies surrounding the regulations. For example,

---

144. *See supra* text accompanying note 131.

145. *Junger*, 8 F.Supp.2d at 716 (N.D. Ohio 1998) (citing Texas v. Johnson, 491 U.S. 397, 404 (1989)).

146. *Id.* at 717.

147. Amicus Brief at 11, Bernstein v. U.S. Dep't of Commerce, 974 F.Supp. 1288 (9th Cir. 1997) (No. 97-16686).

most (if not all) of the encryption source code at issue in the cases is already available on the Internet from non-U.S. sites.[148] This makes any regulation prohibiting the exportation of encryption ineffective, because the goal of the current regulations is not to inhibit domestic use of encryption, but rather to prevent the exportation of encryption to foreigners.[149] The fact that much of the encryption can be obtained from non-U.S. sites is also important because many of the bills currently in Congress would under such circumstances allow for the encryption to be exported.[150] Another unresolved issue arises from the fact that most commercial encryption products are sold in object code form and not in source code.[151] The *Bernstein* decision however, only held that "high level" computer languages constituted speech, but did not decide whether "low level" languages such as object code also constituted speech.[152] All of these issues should be addressed by future regulations if they are to be successful.

Furthermore, the *Bernstein* decision is also not quite the victory that many encryption advocates believe it to be since the decision only affects the current regulations. The current regulations could be modified or new regulations put in place that could restrict the exportation of encryption and yet still satisfy the *Freedman* test. In other words, the *Bernstein* decision was based upon "curable defects" of the current regulations.[153] The Commerce Department could for example, create standards which require a reasonable and specific time limit upon which the licensor must make a decision and that would provide for prompt judicial review. Therefore, if the administration and the Commerce Department decide to maintain the current level of restrictions, but provide the necessary standards for decision making and review, exporters and privacy advocates are not likely to be as satisfied with the *Bernstein* decision as they were initially.

Presently, *Bernstein*, *Karn*, and *Junger* only add uncertainty to regulations that were already complex and confusing to those companies who desire to export products containing encryption. Few concrete answers are provided to companies who would prefer to have definitive rulings upon which to base their business decisions and further litigation is

148. RUBINSTEIN, *supra* note 3, at 340.

149. *See supra* text accompanying note 5.

150. Sharon Machlis, *House Committee Kills Crypto Controls Amendment*, COMPUTERWORLD, Sept. 29, 1997, at 16.

151. RUBINSTEIN, *supra* note 3, at 340.

152. *Id.* There are those that believe that the analogy between machine-readable code and foreign languages is not very compelling. *Id.* See also note 79 *supra* and the article by Thinh Nguyen to which it refers.

153. Mainland, *supra* note 88.

therefore likely. Although appellate court review of the contrasting approaches of the three cases may eventually result in the clarification of many of these issues, in the meantime they only add to the confusion which has already resulted in a "regulatory nightmare" for both exporters and regulators.[154] In an attempt to resolve this situation there has been an effort by both the executive and legislative branches to create new laws that will more effectively regulate the use and exportation of encryption products. However, given all of the obstacles, it has proven a difficult task to obtain a consensus about what the future regulations should encompass.

IV. DIFFERING OPINIONS OVER ENCRYPTION AND RECENT APPROACHES

The computer industry, financial institutions, and intellectual property owners are at odds with various parts of the government as to how encryption should be controlled as well as to the degree that it should be controlled. On one side of the debate is an unusual alliance of business interests and civil liberty groups, with bipartisan support in Congress, who argue that all encryption export controls should be lifted.[155] This alliance claims that strict controls on encryption software violate the First Amendment and harm U.S. economic interests by allowing companies from other countries to dominate the market for encryption products.[156] In addition, this side of the debate argues that current controls on encryption fail to protect national security interests because equivalent programs are readily available abroad while simultaneously putting financial systems and valuable intellectual property at risk.[157] On the other side of the debate are the groups that would prefer to bar all powerful forms of encryption technology except for those to which the government is allowed access.[158] These groups argue that this degree of control is necessary to prevent those uses of encryption which assist criminals in endeavors like money laundering and terrorism.[159]

Between the two extremes of complete deregulation and the banning

---

154. *See* Laura M. Pilkington, Comment, *First and Fifth Amendment Challenges to Export Controls on Encryption: Bernstein and Karn*, 37 SANTA CLARA L.REV. 159, 204 (1996).

155. Nicholas W. Allard & David A. Kass, *Law and Order in Cyberspace: Washington Report*, 19 HASTINGS COMM. & ENT.L.J. 563, 574 (1997).

156. *See* MIDDLEHURST, ET AL., *supra* note 6, at 555.

157. *See* RUBINSTEIN, *supra* note 3, at 346. *But see* Stender, *supra* note 4 (article discussing the importance of national security in the encryption debate).

158. Allard & Kass, *supra* note 155, at 574.

159. *Id.* at 573.

of strong encryption is a middle path.[160] Either the EAA might be renewed giving the administration new statutory authority for its EAR amendments or entirely new legislation might be passed that is specifically tailored to deal with the exportation of cryptographic products.[161] The latter seems to be the preferred choice at the present time as evidenced by the number of bills and amendments that are currently winding their way through Congress and would have the added benefit of removing the uncertainty that has arisen from the current litigation as to how the court system will resolve the constitutional issues. In addition, it would be prudent for Congress and the administration to provide procedures that are more likely to satisfy First Amendment challenges within any future regulations that they pass.

A. *The Clinton Administration's Proposals*

For its part, the Clinton administration has put forth a series of proposals that attempt to bridge the two extremes between complete deregulation and banning. One result of these efforts was Clipper IV, which was formalized in November of 1996.[162] It featured the aforementioned transfer of jurisdiction over encryption export licensing from the State Department to the Commerce Department.[163] Clipper IV also originally permitted the exportation of 56-bit encryption products for two years, provided that the computer industry committed itself to building and marketing future products that supported key recovery systems.[164] The industry was also required after two years to have key escrow capabilities installed within all exportable products of greater strength than 40-bits.[165] Finally, Clipper IV encouraged the adoption of key escrow systems through international agreements, standard processes and a new key management infrastructure.[166]

Many in private industry were unhappy with the regulations that were implemented by the Commerce Department subsequent to the transfer of jurisdiction. They were disturbed with the government mandate that products include a key escrow system and were worried that a key

---

160. *Id.*

161. *See, e.g.*, Pilkington, *supra* note 154, at 204.

162. *See, e.g.*, Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM.U.L.REV. 967, 994 (1997).

163. *Id.* at 995.

164. *Id.*

165. *Id.*

166. *Id.*

escrow system would be too complex for consumers.[167] Another criticism is that companies would be "required to submit business and marketing plans as conditions for export."[168] Although, some of these complaints were addressed by the administration's decision to loosen the regulations in September, 1998, many criticisms still exist.[169]

The biggest complaint still expressed by private industry over the regulations is that the controls will create a significant competitive disadvantage for U.S. companies and may force the U.S. computer industry to lose an important market to foreign rivals.[170] The Economic Strategy Institute (ESI) has estimated that if current U.S. encryption policies are not reformed, the potential lost revenues for the U.S. information industry could reach $35-$95 billion over the next five years.[171] The ESI study also found that 1,601 encryption products were available from 941 firms in 30 countries as of September 1997.[172] Of these, 653 products were manufactured outside of the United States by 472 foreign firms.[173]

However, the view that encryption regulations will harm the U.S. computer industry is not universally accepted. Commerce Under Secretary William Reinsch, has written that "export controls will help maintain U.S. market share of future encryption."[174] Reinsch wrote that voluntary registration of certificate authorities and key-recovery agents will lend credibility to encryption services and help to ensure clients that minimal responsibility standards have been met.[175] Reinsch also stated that

---

167. *See* Allard & Kass, *supra* note 155, at 576.

168. *Id.*

169. *See supra*, notes 14-15 and accompanying text; John Simons & David Bank, *Restrictions Are Relaxed on Encryption Exports*, WALL ST.J., Sept. 17, 1998, *available in* 1998 WL-WSJ 18984704.

170. *See* MIDDLEHURST, ET AL., *supra* note 6, at 555; Corcoran, *supra* note 32.

171. *Study: U.S. Will Lose $35-95 Billion Due to Encryption Controls*, 12 NEW TECH. WK., Apr. 13, 1998, *available in* 1998 WL 9047819 (hereinafter *Study*). *See also* James B. Altman & William McGlone, *Demystifying U.S. Encryption Export Controls*, 46 AM.U.L.REV. 493, 510 (1996). The Commerce Department estimated that by the end of 1997 there were 656 different types of encryption products available in 29 countries. *Administration's Encryption Policy Is "Failure," Secy. Daley Admits*, TR DAILY, Apr. 15, 1998, *available in* 1998 WL 6571617 (hereinafter *Administration*).

172. *Study*, *supra* note 171, at 510.

173. *Id.*

174. Symposium, *Q: Should Uncle Sam Control U.S. Encryption Technology Exports? SUBH: Yes: Export Controls Will Help Maintain U.S. Market Share of Future Encryption Products*, INSIGHT MAGAZINE (Sept. 8, 1997) (hereinafter *Symposium*). However, see *supra* the text accompanying note 27 for a more recent statement by William Reinsch in regards to the license exception given to Cylink which seems contradictory in that the exception permits Cylink to export without promising key recovery.

175. *Id.*

encryption products are going to be most in demand when the infrastructures within which they can function are in existence and that unrestricted sales abroad will not make businesses more competitive.[176] While key recovery may indeed lend some credibility to an encryption product, encryption's greatest asset to consumers and to electronic commerce is that it makes business transactions more secure and eliminates concerns that private information may end up in the hands of criminals. Therefore, as long as the United States restricts the exportation of the strongest encryption within products while other countries do not, it is likely that U.S. companies will lose market share to foreign corporations which will force U.S. companies to either not participate in foreign markets or use foreign encryption products in order to do so.

B. *Legislative Proposals*

In response to these criticisms, various members of Congress have proposed their own solutions to reform the encryption exportation regulations. Some of these bills are designed to loosen controls while others would make the exportation of encryption more difficult. One of the most prominent is H.R. 695, the Security and Freedom through Encryption (SAFE) Act.[177] As originally introduced in 1997, this bill proposed removing encryption software from current U.S. export controls.[178] The original bill would have prohibited mandatory key escrow, allowed Americans to use any encryption software, placed export control with the Commerce Department, allowed encryption software to be exported if similar products were available overseas and made the use of encryption for criminal purposes illegal.[179] However, as this bill made its way through the five committees that have jurisdiction over encryption, various restrictions upon exportation were added to create what were essentially entirely new and diametrically opposite versions of the original bill.[180]

One of these committee amendments was the Oxley/Manton proposal which represented the FBI's position and would have required encryption software to include key recovery techniques for police investigators through a "backdoor."[181] This contradictory version of the SAFE bill

176. *Id.*

177. H.R. 695, 105th Cong. (1997).

178. John Rendleman, *Encryption Conniption: E-Commerce Users and Vendors Decry Effort to Tighten Controls*, INTERNET WEEK, Sept. 22, 1997, at 1, 76. The bill was introduced by Congressman Goodlatte (R-Va.). Machlis, *supra* note 150, at 16.

179. Machlis, *supra* note 150, at 16.

180. Rendleman, *supra* note 178, at 1, 76.

181. Jim Barksdale, *Washington May Crash the Internet Economy*, WALL ST. J.,

which has been sarcastically referred to by opponents as the "UNSAFE" bill would have required all encryption products, even those sold or distributed in the United States after January 31, 2000, to include a key recovery system.[182] This proposal and others that are similar have been advocated by law enforcement agencies but vigorously opposed by private industry and privacy advocates.[183]

One of the least restrictive proposals was put forward by Senator Conrad Burns from Montana. His proposal would have limited the enactment of any regulation resulting in encryption standards to those systems operated by the federal government.[184] The proposal would also have prohibited regulations intended to impose government-designed encryption standards on the private sector.[185] Finally, the proposal would have prohibited regulations that restrict the sale of any product with encryption capabilities or that require that encryption products contain a mandatory key escrow system as a condition of sale.[186]

By the end of September 1998, no versions of the SAFE bill or any of the other bills had made it to the floor of the House and similar legislation was stalled in the Senate.[187] Even though all of the bills have stalled in committees, they do have some things in common. For instance, they would increase the penalties for the use of encryption for illegal activities and would leave control over encryption exportation with the Commerce Department. However, these similarities are minor in comparison to the number of other areas of disagreements and the conflicting viewpoints held in respect to those areas. The biggest obstacle involves the disagreements over the possibility of a mandatory key escrow

---

Sept. 26, 1997, at A22, *also available in* 1997 WL-WSJ 14167840. Another potential problem that may result from the FBI plan is more crime. *See id.* The FBI proposal "would expose computer users to assault by hackers intent on economic espionage, blackmail and public humiliation." *Id.* For example at one congressional hearing, a witness testified that "with $1 billion and 20 people using existing technology, he could effectively shut down the nation's information infrastructure, including all computer, phone and banking networks. Another witness said he could do it for $100 million." *Id.*

182. Alan J. Hoffman & Eric H. Vance, *Sides Debate Future of Encryption: Easy Answers Hard to Find Privacy Advocates, Law Enforcement at Odds*, N.Y.L.J., July 13, 1998, at S7.

183. *See, e.g.*, Rendleman, *supra* note 178, at 12. However, the FBI's position does have its supporters in Congress. Senator Dianne Feinstein (D-California) has stated that "nothing other than some kind of mandatory key recovery really does the job" and that key recovery products should be mandatory domestically as well as internationally. Pietrucha, *supra* note 5.

184. Allard & Kass, *supra* note 155, at 578.

185. *Id.*

186. *Id.* at 579.

187. Kerstetter, *supra* note 2, at 16.

system, with whom keys would be placed, and when they would be given to the government. Many people are opposed to mandatory key escrow systems and are wary of placing the keys in the hands of the government or third parties because of the potential for misuse.[188] Although the government has stated that it does not want direct control of the keys, preferring instead for third parties to control the keys,[189] many people in private industry as well as privacy advocates are adamantly opposed to any form of mandatory key escrow.[190] However, privacy advocates and industry are themselves not always in complete agreement. Many in private industry seem more willing to make some concessions which are not supported by privacy advocates.[191] Most people in private industry are willing to accept provisions that would make it a crime to use encrypted communications in the commission of a felony, whereas, most privacy advocates find this unacceptable.[192] Privacy advocates such as Ms. Sehgal of the ACLU argue that it is unconstitutional to "create [a crime that is] based on the use of technology where the crime [itself] is not related to the technology."[193]

Another area of disagreement is that some people within the government want real-time access to all encrypted data without having to notify the user.[194] They argue that this would essentially allow the government to access such encrypted communications after obtaining a court order, a practice that is similar to what is currently done with telephones.[195] However, there is a fear within private industry that requiring real-time access would hinder the rise of electronic commerce.[196]

---

188. *Id.* at 16, 18.

189. Symposium, *supra* note 174, at 151. "The Clinton Administration consistently has stated that the government does not wish to hold the keys to encrypted communications." *Id.*

190. Kerstetter, *supra* note 2, at 16. Many in the computer industry have pointed out that any key escrow system is bound to create problems. They worry that key escrow systems are susceptible to criminal hacking efforts and also that employees of escrow companies themselves might also be able to steal crucial keys either to sell to criminals or as the result of blackmailing efforts. John J. Fried, *Code of Contention, Controversy Over Internet Encryption Has Factions Deciphering Issues of Privacy, Crime And Security*, HOUSTON CHRON., Apr. 24, 1998, *available in* 1998 WL 3573510.

191. *See* Alan Cohen, *Sides Talk Compromise, But Encryption Policy Lags, Deadlock May Be Harder to Break Than Codes Themselves*, 219 N.Y.L.J. at S3 (1998).

192. *Id.*

193. *Id.* The creation of this type of offense has the potential for being a very powerful weapon for a prosecutor in a plea bargain. *Id.*

194. *See, e.g.*, Kerstetter, *supra* note 2, at 16.

195. *Id. See* Stender, *supra* note 4.

196. *See, e.g., id.*

Addressing these concerns is one of the most recent bills, S.2067, that was introduced by Senators Patrick Leahy (D-Vermont) and John Ashcroft (R-Missouri).[197] This bill, called the E-Privacy Act, would permit U.S. companies to export products, as well as most software and hardware, containing strong encryption without key recovery requirements as long as there is a competing foreign product that is already or imminently available.[198] The bill would also not place any restrictions upon the use of any level of encryption within the United States.[199] Furthermore, the bill would create a National Electronic Technologies Center which would assist law enforcement agencies in obtaining expertise in encryption technology.[200] Although the bill prohibits the mandatory escrow of decryption keys, it does allow law enforcement officials access to decryption keys under existing wiretap authority and would allow them to obtain keys or third party assistance for remotely stored data with a court order or subpoena.[201] This bill is a compromise between the interests of private industry and law enforcement agencies, because it allows the industry to compete with foreign businesses by easing restrictions while simultaneously giving law enforcement officials the right to obtain keys whenever they have probable cause.

V. ENCRYPTION CONTROLS OVERSEAS

The domestic issues surrounding the encryption regulations are not the only concerns facing the U.S. government's export policy. Problems will also arise if the United States implements regulations unilaterally rather than as part of a broader multinational effort.[202] If regulations are implemented unilaterally, they will be ineffective in controlling wide-

---

197. S.2067, 105th Cong. (1998). *See, e.g., id.* The bill contains a "mass market" provision that would allow for encryption products to be exportable under a license exception if they are generally available off the Internet or retail shelves. Charlotte Dunlap, *E-Privacy Act: Would Allow U.S. Companies to Better Compete Abroad*, COMPUTER RESELLER NEWS, May 25, 1998, at 109, *available in* 1998 WL 11981745.

198. *See, e.g.*, Bill Pietrucha, *Senators Introduce New Encryption Bill To Ease Limits*, NEWSBYTES, May 12, 1998, *available in* 1998 WL 11721982.

199. *See, e.g.*, Bill Pietrucha, *Senators Introduce New Encryption Bill To Ease Limits*, NEWSBYTES, May 12, 1998, *available in* 1998 WL 11721982.

200. *Id.*

201. *Id.*

202. "Because of the Internet's borderless nature, American officials have long acknowledged that their plan [for "key escrow"] was workable only if most other countries adopted similar systems. If not, people could simply route their communications through countries with no restrictions." Edmund L. Andrews, *Europe Rejects Computer Plan: U.S. Wants Key to Crack Codes*, SEATTLE POST-INTELLIGENCER, Oct. 9, 1997, at C1, *also available in* 1997 WL 3209807.

spread use of strong encryption, U.S. companies will purchase encryption products from overseas, and U.S. producers of encryption will lose business to overseas competitors.[203] The Clinton administration has realized this and has attempted to coordinate U.S. action with that of other nations by organizing meetings of encryption experts through the Organization for Economic Cooperation and Development (OECD) in an effort to obtain broader international acceptance of U.S. key escrow proposals.[204] But creating a global encryption policy is obviously easier said then done. Currently there is not a consensus among nations as to what degree, if at all, encryption should be regulated.[205] For example, although 33 countries have some controls over the exportation of encryption products, only a few countries agree with the United States that key escrow should be included within encryption products.[206] The United States also extends its encryption controls to software that contains encryption, but is one of only a few countries to do so.[207] It is therefore necessary to describe the current policies of other countries to determine the type and scope of regulations that might be possible in the future.

---

203. Altman & McGlone, *supra* note 171, at 510. "At a more fundamental level, the availability of cryptographic software outside the United States underscores the futility of overly restrictive unilateral export controls. In today's global marketplace, geographic boundaries present fewer and fewer barriers to trade. Thus, now that the business world is linked electronically, U.S. restrictions arguably will drive the restricted activities outside the United States without limiting the development or dissemination of the >controlled' technology." *Id.* Currently a third of the sites run by non-U.S. companies are capable of 128-bit encryption. *Encryption Ban "No Real Worry" Outside U.S. Business,* IRISH TIMES, Feb. 23, 1998, at 10, *available in* 1998 WL 6227838.

204. *See, e.g.,* MIDDLEHURST, ET AL., *supra* note 6, at 557. But while Canada will be hosting a meeting of the OECD this fall to set rules for electronic commerce, encryption issues are not on the agenda. Jill Vardy, *Insecurity Complex: Promise of E-Commerce Stalled by Paranoia as U.S. Fears Encryption Technology Could Fall Into Criminal Hands,* FIN. POST, May 2, 1998, at 12, *available in* 1998 WL 10760190.

205. Stewart A. Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions, in* DOING BUSINESS ON THE INTERNET, at 287, 301-02 (PLI Patents, Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. G4-3988, 1996). The lack of consensus is understandable considering that at the end of 1997 there were 656 different types of encryption products available in 29 countries. *Administration, supra* note 171.

206. *See* Vardy, *supra* note 204. A recent survey of 230 countries by the Global Internet Liberty Campaign showed that eight nations are definitely in support of a key recovery system. Lisa S. Dean, *U.S. Encryption Policy Difficult to Decode,* SEATTLE TIMES, Apr. 21, 1998, at B5, *available in* 1998 WL 3149397. The eight nations that also desire a key recovery system are China, France, India, Israel, the Republic of Korea, Pakistan, Russia and Singapore. *Id.*

207. *See* Vardy, *supra* note 204.

France has some of Europe's toughest laws on encryption[208] and has been supportive of key escrow policies for encryption.[209] For products with encryption capabilities, French businesses are required to file with the government.[210] There is also a proposed amendment in France that would restrict the import, use or sale of encryption products unless an encryption key is escrowed with an escrow agent that has been approved by the French government.[211] Great Britain and Israel are two other countries that favor encryption regulations. Britain also is supportive of key escrow and has generally sided with the United States in supporting an international regime for regulating data encryption.[212] Israel currently requires a license for the import, export, production or use of any encryption product.[213]

Russia has also implemented a highly regulated framework for encryption technology that requires licenses for most activities involving encryption including the import of products with encryption capabilities.[214] This decree has been highly criticized within Russia for a number of reasons, including concerns that it is over broad and a violation of civil rights.[215] But even though the Russian regulations may appear stringent, there has been very little enforcement of the existing measures.[216]

In China, companies are required to obtain licenses in order to import or export encryption.[217] The available evidence indicates that approval for the use of encryption products is not necessarily easy to obtain.[218] However, China is not likely to join in an international consensus on encryption policy given their past disagreements over arms proliferation and human rights practices and since they have not yet sent any representatives to the major international meetings on encryption.[219]

Although Canada has historically had similar export regulations to the United States and is the one country that encryption can be exported to from the United States without a license, it is now considering imple-

---

208. Kimberly A. Strassel, *Secret For Success: Europeans Unlock Encryption Market, Thanks to U.S. Rules*, WALL ST. J. EUR., June 30, 1998, at 1, *available in* 1998 WL-WSJE 12725941.

209. BAKER, *supra* note 205, at 303.

210. MIDDLEHURST, ET AL., *supra* note 6, at 556.

211. *Id.*

212. *See* Andrews, *supra* note 202, at C1.

213. *Id. See* Baker, *supra* note 205 at 303.

214. MIDDLEHURST, ET AL., *supra* note 6, at 556-57.

215. *See id.* at 557.

216. *See* BAKER, *supra* note 205, at 303.

217. *Id.* at 304.

218. *See id.* at 305.

219. *See id.*

menting more liberal regulations that would allow for the exportation of stronger levels of encryption.[220] As for key recovery, Canada is still deciding whether to have it be discretionary or whether to make it mandatory.[221] In an attempt to resolve these dilemmas Canada has created a task force to outline the potential levels of control while trying to balance the security concerns of law enforcement with the market demands of businesses.[222] This task force, the Canadian Task Force on Electronic Commerce, accepts public comments and solicits input on what direction Canadian policy should take.[223] Although Canada realizes that liberalizing its export controls could bring about pressure from the United States, it is also fearful of losing market share to European firms.[224]

In Japan, the government is currently studying the export problem but is reportedly suspicious of key escrow which they view as a possible method of allowing U.S. businesses to dominate the market for electronic commerce.[225] The German government, like its Japanese counterpart, is worried that U.S. business might dominate the market and that American authorities might have improper access to data on German users.[226] Germany is also concerned that this access might violate Germany's laws on data protection.[227]

While the previous countries have been relatively open to the idea of encryption regulations, if not key escrow, there are still some countries such as Ireland, Switzerland, and Finland which are very liberal toward the use and regulation of encryption.[228] Nevertheless, there are signs that some of these governments are beginning to believe that international coordination on an encryption policy is necessary to prevent the widespread international deployment of strong encryption.[229] Although it is possible that this coordination might result in an international commer-

---

220. *Canada Mulls Liberal Encryption Exports: Neighbor Wary of Irking United States*, 3 ELECTRONIC COMMERCE NEWS, Apr. 6, 1998, *available in* WL 7200513 (hereinafter *Canada Mulls*). Canada now permits Canadian businesses to export 56-bit products. *Id.*

221. *Id.*

222. *Id.*

223. *Id.*

224. *See id.* Helen McDonald who is the director general of policy development for the task force has said that "we're watching what you guys [the United States] are doing because we're big trading partners. [B]ut if somebody's going to open their gates and flood the market [with strong encryption], it's hard to go the other way." *Id.*

225. *See* MIDDLEHURST, ET AL., *supra* note 6, at 556.

226. *See* Andrews, *supra* note 202, at C1. *See* Strassel, *supra* note 208.

227. *See id.*

228. *See Canada Mulls, supra* note 220.

229. *See* Baker, *supra* note 205, at 306.

cial key escrow system, this outcome is unlikely since such a system would require an unprecedented degree of government coordination and would need to provide a means for a foreign government to receive a surveillance target's keys from a foreign escrow agent.[230] In addition, although many countries in Europe and Asia believe in some form of key escrow, they are working more closely with the software community than is the U.S. government and appear to recognize the limits of access.[231]

Recently, the European Commission rejected proposals by the United States that called for the creation of an international key escrow system.[232] The European Commission was concerned that the U.S. approach might threaten privacy, stifle the growth of electronic commerce, and ultimately be ineffective because hackers might find new ways to breach security.[233] Even if a key escrow system were to be put in place, the European Commission was not convinced that criminals could be entirely prevented from using strong encryption.[234] Several European countries also do not like the idea of deferring to an American system that might allow American companies to dominate the market for security products.[235] However, the European Commission's action does not block member countries from setting up key-based systems on their own.[236] Thus, it is still possible for the United States to work with individual European nations, though this obviously does not go as far toward creating a global policy regarding encryption as would a plan endorsed by the entire European Union.

In addition to the critiques put forth by the European Commission, another issue that will make it difficult for individual nations to come to a key escrow agreement involves the dilemma of who would be responsible for holding the keys. There are several possibilities, each of which contains its own inherent problems and limitations that would have to be resolved before they could be successfully implemented. For example, it seems unlikely that nations would allow any other nation to hold the keys for businesses located outside of their nation. Another possibility is that the keys could be divided and given to the different nations involved. Although, this would presumably prevent the inappropriate use of the keys, it would also require a great deal of interaction between the na-

---

230. *Id.* at 307.

231. Jim Kerstetter, *Encryption Battle Not as Heated Overseas*, PC WEEK, Oct. 6, 1997, at 35.

232. Andrews, *supra* note 202, at C1.

233. *Id.*

234. *Id.*

235. *Id.*

236. Andrews, *supra* note 202, at C1.

tions because both nations would have to agree when to use the keys and would therefore probably result in a level of bureaucracy that would be unduly burdensome. A third possibility is that the keys could be placed in the possession of an international agency, though once again the problem arises that many countries would not agree to give up control of the keys.

These difficulties are obviously a major setback to the Clinton administration's effort to establish a global key escrow system. As is the issue of how to deal with those nations who are opposed to exportation regulations and those who do not want to cooperate in an international setting. With this setting of disagreement and suspicion, it is unlikely that a consensus will arise among most nations in the near future. But as the U.S. government has acknowledged, if the export restrictions are going to be successful, something must be done on a global scale relatively soon.[237] Although the United States acknowledges the necessity of coordinating policies with foreign governments if future regulations are to be successful, the United States continues to put together a "mosaic of regulations" that lets some companies sell sophisticated products to certain users under certain conditions.[238] While these piecemeal approaches produce some beneficial results, they do not eliminate the eventual need for exportation regulations to be coordinated with those of other countries if the regulations are to be effective in the long-run.

VI. A MULTI-TIERED INTERNATIONAL APPROACH

Because of the widespread international availability of advanced encryption algorithms, the United States can no longer control, to the same degree that did in the past, the encryption strength used and acquired by the rest of the world. As encryption use spreads further, unilateral approaches by individual countries will become unworkable, and an international consensus will be required if future encryption regulations are going to succeed. Furthermore, given the conflicting interests of civil libertarians, businesses, and law enforcement, the differing importance of each of these groups within each country, and the dissimilar treatment of

---

237. Undersecretary of Commerce William Reinsch has conceded that the exportation ban on encryption software is on shaky ground because U.S. policy has not been backed by foreign governments. Reinsch also stated that "if we can't get our allies to do the same kind of thing we're doing, in a year or so we'll have to review this." *Encryption Export Ban Tested; But Shipments Across Europe May Violate U.S. Law*, BALTIMORE SUN, Mar. 21, 1998, at 15C, *also available in* 1998 WL 4957233.

238. Elizabeth Corcoran, *Breakthrough Possible in Battle Over Encryption Technology*, WASH. POST, July 12, 1998, at A8, *available in* 1998 WL 11591560.

encryption by countries in the past, it is difficult to imagine that any one rigid level of encryption could be agreed upon for all types of transactions in all countries.

A multi-tiered approach is therefore more realistic than a unilateral one and has a better chance of meeting diverse national and local business objectives. To be successful a multi-tiered approach should have well-defined categories based upon the type of user, the country of destination, and the value of the message content. Such an approach would be more appealing to other nations and more likely to gain international approval because it is inherently better suited to accommodating the differing needs and concerns of the various nations. Consensus could be built by having an international organization or conference work out the specifics of each tier. One possible plan is presented below and would encompass three tiers representing different security requirements.

A. *The First Tier*

The first and strongest encryption tier would allow at least those service industries for which the U.S. government presently has granted exceptions, such as financial, medical, and insurance to use the highest level of encryption possible without requiring either key escrow or a backdoor. This use would be subject to strict guidelines that are comprehensive and explicit. Before being permitted to use the encryption, businesses could be required to register what they are using the encryption for and the various localities in which they will be using it. This is similar to what is currently being allowed both by the United States and elsewhere but would have the advantage, at least in the United States, of making the regulations controlling such use uniform and explicit rather than being administered and changed on an ad hoc basis.

B. *The Second Tier*

The second tier would include stand-alone encryption used internationally by private industry. This tier would be a hybrid of the first and third tiers and allow a level of encryption, such as 96-bit, that is stronger than the third tier but weaker than the first. The owners of such encryption would be required to register with their respective countries. This tier would allow businesses that do not qualify for the first tier to use a level of encryption that would allow them to keep their trade secrets and communications confidential. Each country could require that the businesses located within its territory use some form of key escrow and that communications between businesses of different nations use key escrow if one of the respective countries requires the use of key escrow. A country normally requiring key escrow would be able to enter into bi-lateral

agreements with other countries that would allow the businesses of the two countries to communicate with one another without the use of key escrow, such as is currently being done between the United States and Canada. This approach is more likely to appeal to governments, because it would allow them to decide when key escrow would be required and for which countries, but would still provide benefits to industry by presumably allowing them greater flexibility in their exports to more nations than under the current regulations by decreasing the number of countries for which licenses would be required. In terms of product development, this approach may cause difficulties, because for some countries key escrow would be required while for others it would not be, thus creating the need for a product that would be able to either use or not use key escrow from one application to the next.

There are however, other possibilities as to how this mid-level security tier might be structured. Recently, a coalition of high-technology companies announced a plan, dubbed the "private doorbell," that could comprise the second tier.[239] In its current form this plan affects private companies and Internet service providers who serve as gateways for managing the electronic messages sent by their employees or their subscribers.[240] Under the "private doorbell" plan, law enforcement officers following a warrant could pull out specific messages either just before the product or network scrambles outgoing mail or just after the incoming mail is deciphered.[241]

This plan would therefore prevent both the government and outside hackers from intercepting the data while it is in transit either over the Internet or a private network using the companies' products.[242] While the plan is supported by many in the U.S. business sector, it is not known whether other national governments would agree to such a plan. As for the United States government, the Commerce Department has stated that the plan "raises serious issues that must be considered."[243] For instance, the plan does not address the issue of how the networks will protect the messages from outside hackers and corrupt employees while they are in their less protected state.[244] Furthermore, for overseas communications, U.S. law enforcement would need to have the cooperation of the local

---

239. *Id.*

240. *Id.*

241. *Id.*

242. *10 Companies Propose Encoding With Legal Access: Export Approval Sought for 'Private Doorbells,' Corporate Security*, BALTIMORE SUN, July 14, 1998, at 3C, *available in* 1998 WL 4975660 (hereinafter *10 Companies*).

243. *Id.*

244. Corcoran, *supra* note 238.

authorities as well as the relevant network managers in order to access information.[245] This is similar to what law enforcement currently has to do when they monitor telephone calls.[246] Although U.S. domestic law enforcement agencies appear willing to accept this proposal, the National Security Agency (NSA) has expressed strong opposition to the plan because it currently can eavesdrop on overseas communications without obtaining permission from anyone.[247] Government agencies are also not the only groups that have expressed their concern over the proposal. Privacy advocates have criticized the "doorbell" approach as being more useful to big businesses than to ordinary Internet users.[248] These issues will have to be resolved before approval of the plan, a process that is likely to take quite some time given the nature of the debate and the concerns that the government has about the plan.

C. *The Third Tier*

The third tier would include users of mass market telecommunications such as telephones, faxes, and e-mail that would be limited to 56-bit encryption. This would be enough protection for most ordinary, non-criminal uses of such technology and provide a sufficient deterrent to non-government interception of these communications.[249] Such a level of encryption would provide more security then is typically currently used for such communications while not an overly high level that the government would not be able to crack it if it were deemed necessary to do so. This tier would also include some form of universal key escrow since it would be more acceptable to the international community then would key escrow for the first tier or second tier. Limiting the level of encryption to 56-bits for this tier does not mean that the users within this tier have fewer rights than those in tier one or tier two. Rather, it is a compromise position that acknowledges that the reasons for allowing persons within tier three stronger encryption are not as persuasive as are the reasons for providing those in the first two tiers, since the incentives for hacking the transmissions of tier three are not as great as the other two tiers and the

---

245. *Id.*

246. *Id.*

247. *Id.*

248. *10 Companies*, *supra* note 242.

249. *See supra* note 2 (illustrating how long it would take to break a 56-bit key and the amount of money it would require).

consequences of a successful hacking are arguably not as severe in tier three.

VII. CONCLUSION

The exportation of encryption is currently governed by a complex and confusing set of regulations that produces arbitrary results and may also violate the First Amendment. Even though it is likely that the First Amendment concerns will be resolved by the courts in a manner that will relax the current controls, the Presidential administration and Congress, if they so desire, could maintain the same level of export restrictions by including more procedural safeguards within the licensing process. But, not only do the current regulations suffer from this malady, they are also the target of other criticisms from parties familiar with the debate. Many in the computer industry would like to have less comprehensive regulations, while law enforcement agencies such as the FBI and the NSA would prefer restrictions that would allow them access to all encrypted communications, both domestic and foreign. Although there are groups between these two extremes, there has yet to arise a consensus on what future regulations should encompass. Instead the government and industry seem intent on proposing piecemeal approaches that are designed to only address specific areas of the impasse. The sheer number and breadth of these continuous proposals are indicative of how quickly this field is changing and of how difficult it will be for the various sides to come to an agreement.

Complicating matters even further is that any unilateral action taken by the United States is unlikely to be successful. Currently international uniformity does not exist and while a multi-tiered approach might provide a way to overcome this, it does not appear as if the present impasse is going to change in the near future. The complexity and confusing nature of the U.S. regulations and the lack of uniformity among regulations worldwide is unfortunate because it creates an atmosphere of uncertainty. This uncertainty is undesirable from a business perspective because it forces companies to make decisions based upon fluctuating worldwide market conditions. Such a situation may ultimately either leave companies vulnerable to liability by unknowingly violating U.S. or foreign encryption regulations or even compel them to forgo legal exports because of complicated and costly regulations.

E. Franklin Haignere