WHERE THE UNITED STATES GOES THE WORLD WILL FOLLOW—WON'T IT?

TABLE OF CONTENTS

I. INTRODUCTION

To compete in the rapidly emerging global economy, business and commerce must have strong encryption schemes, available on an international basis, to protect the confidentiality and integrity of business transactions and electronic commerce.[1] The U.S. encryption industry dominates the market for encryption technology, but its lead may be diminishing.[2] The U.S. encryption industry stands poised to lose its competitive edge to foreign encryption industries,[3] which some think will result in the loss of thousands of jobs and millions of dollars in revenue.[4] International and domestic debates on the regulation of encryption technology have reached a crescendo. The purpose of this comment is to clarify the debated issues, as well as to encourage industry to abandon its insistence on a total abrogation of regulation of encryption technology, and to work with the Clinton Administration to develop a compromise.

Part II of this comment provides a quick tutorial on encryption. Part III describes the competing arguments for and against regulation, in the form of "key management." Although presented from the U.S. perspective, these

---

1. *See* U.S. DEP'T OF COMMERCE & NAT'L SEC. AGENCY, A STUDY OF THE INTERNATIONAL MARKET FOR COMPUTER SOFTWARE WITH ENCRYPTION III-5 to III-6 (1996) [hereinafter EXPORT STUDY].

2. *See id.* at ES-2.

3. *See id.* at III-25.

4. *See Letting the Internet Flourish*, WASH. TIMES, July 3, 1997, at A16 (editorial).

arguments mirror the struggles taking place in other countries that are formulating their own encryption policies.[5] Part IV discusses how the United States is regulating encryption technology. This section specifically examines the internal discord in Congress over regulation of encryption technology. Part V compares how other countries and multinational organizations are cultivating encryption policy. Part VI concludes that the encryption industry must take immediate action to maintain its competitiveness, which can be achieved by working with, rather than against, the Clinton Administration.

II. A TUTORIAL: THE KEY TO ENCRYPTION

Encryption is a technique for encoding information that allows only a person possessing an appropriate electronic key to decode it.[6] The information is first scrambled using a mathematical function called an algorithm.[7] The algorithm lets an individual select a "key" that is used to encrypt the information.[8] The "algorithm can be either a 'secret key' algorithm or a 'public key' algorithm."[9] Secret key cryptography uses the same secret key for encryption (sender) as for decryption (receiver).[10] Public key cryptography uses different keys for encryption and decryption.[11] One key is kept private while the other, the public key, can be published in directories.[12] A sender obtains an intended recipient's public key and uses it to encrypt a message.[13] The recipient uses his private key to decrypt the message.[14]

---

5. *See* COMMITTEE TO STUDY NAT'L CRYPTOGRAPHY POLICY, NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 431–33 (Kenneth W. Dam & Herbert S. Lin eds., 1996) [hereinafter CRISIS STUDY].

6. *See* Stewart A. Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions*, *in* DOING BUSINESS ON THE INTERNET: THE LAW OF ELECTRONIC COMMERCE 287, 289 (PLI Patents, Copyrights, Trademarks & Literary Property Course Handbook Series No. G-452, 1996).

7. *See id.* at 290.

8. *See id.*

9. *Id.*

10. *See id.*

11. *See id.* at 291.

12. *See id.*

13. *See id.*

14. *See id.*

Secret key encryption works like this. Amanda wants to send Peter an encrypted message so together they obtain a secret key. Amanda encrypts her message with the secret key and Peter uses the same key to decrypt the message. If Dan the FBI agent wants to read Amanda's messages, he obtains the proper authorization, such as a Title III judicial wiretap authorization,[15] to monitor Amanda's e-mail. With this authorization he obtains Amanda's secret key from the escrow agent. Dan can then read all messages originated by Amanda.

It is possible to decode the message without the secret key by using brute force.[16] Brute force is a decoding method that uses a modern high speed computer programmed to try every possible key combination until it detects the correct one.[17] The longer the key combination the more time and resources it takes to break the code through brute force.[18] The length of the key combination is measured in bits.[19] After a one-time review, U.S. companies in certain industries may export encryption products of fifty-six bits without key recovery.[20] Other U.S. companies may export encryption products of any strength if a third party may recover the key or plain text.[21]

Under the current export regulations, the encryption user must store crypto keys so they will be available if needed for criminal or security investigations.[22] One such

---

15. *See* 18 U.S.C. § 2516 (1994).

16. *Compare* MATT BLAZE ET AL., MINIMAL KEY LENGTHS FOR SYMMETRIC CIPHERS TO PROVIDE ADEQUATE COMMERCIAL SECURITY (1996) (text available at the *Houston Journal of International Law*) (claiming that readily available technology makes brute force attacks "both fast and cheap"), *with* COMPUTER SEC. RESOURCE CLEARINGHOUSE, U.S. CRYPTOGRAPHY POLICY: WHY WE ARE TAKING THE CURRENT APPROACH (1996) (text available at the *Houston Journal of International Law*) (suggesting the "operational reality" of government's ability to decode messages greatly lags behind "mathematical theory").

17. *See* BLAZE, *supra* note 16 (observing the technology called Field Programmable Gate Array); *see also* RICHARD M. NUNNO, CONGRESSIONAL RESEARCH SERVICE, ENCRYPTION TECHNOLOGY: CONGRESSIONAL ISSUES 2 (Jan. 14, 1999).

18. *See id.*

19. *See* Baker, *supra* note 6, at 290.

20. *See* Encryption Items, 63 Fed. Reg. 72,156, 72,157 (1998).

21. *See id.* at 72,159, 72,164 (providing for export of encryption products of unlimited strength if they contain key recovery (72,159) and providing for export of recoverable products (72,164)).

22. *See* discussion *infra* Part IV.B.2.

storage technique is Key Escrow.[23] Key Escrow involves distributing the key to a key escrow agent for storage.[24] A variation of Key Escrow is called Self Escrow.[25] As the name implies, under this storage system the user can self-store the key if he can satisfy government standards.[26] Under the Trusted Third Party (TTP) method, a third party to the cryptographic application actually creates and provides the cryptographic keys to the participants, storing a copy for future key retrieval.[27] The Key Recovery Alliance (Alliance), a coalition of international companies, proposes an alternative to key escrow and third party schemes.[28] The Alliance supports developing a recovery scheme that can be used by all cryptographic schemes and has global scalability.[29] This approach eliminates the need to communicate with an outside agent during setup or message encryption and allows the encryption user to maintain the key at all times.[30]

Under any of these key storage alternatives, law enforcement entities may seek to obtain court ordered access to the key through "proper legal process."[31] This provision has fueled heated debate between privacy advocates and supporters of law enforcement.[32]

---

23. *See* NUNNO, *supra* note 17, at 4–5.

24. *See id.*

25. *See id.* at 5.

26. *See id.*

27. *See The Key to Encryption: Ever Heard of Trusted Third Parties and Clipper Chips?,* FOREIGN REP., Nov. 5, 1998, *available in* LEXIS, News Library, Jandef File.

28. *See* International Bus. Mach., *High-Tech Readers to Facilitate Recovery of Encrypted Information Globally* (visited Feb. 22, 1999) <http://www.ibm.com/ security/html/prallim1.html> [hereinafter *High-Tech Readers*]. Key recovery is commonly used to refer in a general manner to all methods of managing a key so that it can be made available at a later date. It is also the term used by the Alliance to refer to a specific method of protecting and recovering a key. *See id.* For the purposes of this paper the broader term "key management" will be used to refer to key escrow, TTP, or key recovery.

29. *See id.*

30. *See id.* (observing that key recovery does not escrow keys with a third party).

31. *See The Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Telecomms., Trade, and Consumer Protection of the House Comm. on Commerce*, 105th Cong. 85 (1997) [hereinafter *SAFE Hearings*] (statement of Jerry Berman, Executive Director, Center for Democracy and Technology).

32. Much of the Clinton Administration's proposal was incorporated into Senate Bill 909. *See* NUNNO, *supra* note 17, at 10. Senate Bill 909 is sponsored by Senators McCain and Kerrey, Chairman and Ranking Member respectively

III. TO REGULATE OR NOT TO REGULATE, THAT IS THE GLOBAL QUESTION

The U.S. government must weigh many competing factors in formulating a comprehensive encryption export regulation policy. These factors include the following: (1) the impact regulation has on the domestic users, (2) law enforcement concerns, (3) industry competitiveness, (4) privacy issues, and (5) freedom of speech. As other nations formulate their own encryption export policies, they struggle with these same concerns.[33] This Part discusses each of these concerns from the perspective of U.S. policy makers.

A. Domestic Users Do Not Feel Secure

The U.S. government does not limit the use of encryption in the domestic market by its citizens.[34] However, the government does restrict the export of encryption technology.[35] One prominent scholar, Michael Froomkin, argues that regulation of encryption exports is in fact regulation of the domestic market because the regulation of the export market will require industry to create two technologies: one for sale in the domestic market and a second for export.[36]

The domestic standard dictates the amount of privacy a user is able to enjoy,[37] for example, communicating via email or banking via computer. The more secure a user feels the more likely the user is to use the Internet for electronic commerce.[38] Because the export standard has stymied the

---

of the Committee on Commerce, which has primary jurisdiction over encryption exports in the Senate. *See id.* Support and opposition to government supported key escrow does not follow political lines, rather law enforcement and privacy ideologies are stronger indicators of who will support and who will oppose key escrow. *See id.* at 3.

33. *See* CRISIS STUDY, *supra* note 5, at 431.

34. *See* A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15, 16–17.

35. *See* Scope of Export Administration Regulations, 15 C.F.R. § 734.2 (1998) (explaining that encryption software is within the scope of Export Administration Regulations).

36. *See* Froomkin, *supra* note 34, at 16–17 (observing that the strong cryptographic products used by U.S. citizens cannot be exported or sold to foreigners).

37. *See id.* at 17 (arguing that the encryption dilemma implicates fundamental issues of trust between the citizens and the state).

38. *See* Joe Kilsheimer, *Security Is Key to E-Commerce*, ORLANDO SENTINEL, Feb. 15, 1998, at H1 (detailing the beginning of an increase in online shopping due to rising consumer confidence in the security of electronic transfers).

domestic development of encryption,[39] domestic users do not feel secure and consequently are not fully exploiting the Internet's capabilities.[40] The domestic demand for key recovery services is expected to explode.[41] While the current market for key recovery services has not matured, many encryption experts believe that key recovery will fuel the growth of electronic commerce and corporate security both domestically and internationally.[42]

B. Industry Competitiveness

Encryption exports are big money for the encryption industry.[43] A study by the U.S. Department of Commerce and the National Security Agency (NSA) estimated worldwide sales of encryption products (both hardware and software) for 1996 alone at $1.8 billion.[44] Over the last several years, the Clinton Administration has proposed various limitations on exports of encryption technology, none of which has succeeded to date in garnering widespread industry support.[45] Opponents of the Clinton Administration's efforts argue that key management will put them at a competitive disadvantage in the global market.[46]

As the industry waits to see what the standard will be for exports, it has allowed the domestic standard to languish.[47] Initially, the rest of the world waited for U.S. action.[48] One

---

39. *See SAFE Hearings*, *supra* note 31, at 85 (statement of Jerry Berman, Executive Director, Center for Democracy and Technology).

40. *See id.* (explaining that the Internet has still not reached its full potential because of the remaining skepticism toward the confidentiality of electronic transfers).

41. *See* David Mulholland, *Strong Encryption Software Market Foreseen*, NEW TECH. WK, June 2, 1997, at 1. "[A]s electronic commerce grows and the need for corporate security increases, companies will need to be able to regain access to encrypted data when the encoding key has been lost or destroyed." *Id.*

42. *See id.*

43. *See* EXPORT STUDY, *supra* note 1, at III-1. The exact dollar figures are disputed. *See SAFE Hearings*, *supra* note 31, at 56 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce).

44. *See* EXPORT STUDY, *supra* note 1, at III-1.

45. *See* Froomkin, *supra* note 34, at 24–42 (arguing that devices such as the clipper chip software and key escrow are bureaucratic innovations).

46. *See* Rajiv Chandrasekaran, *Freeh Seeks Encryption Decoding Key*, WASH. POST, Sept. 4, 1997, at E1.

47. *See SAFE Hearings*, *supra* note 31, at 82 (statement of Jerry Berman, Executive Director, Center for Democracy and Technology).

48. *See* Froomkin, *supra* note 34, at 60.

commentator has suggested that foreign governments avoided the issue.[49] Foreign governments "had less need for an explicit ban on strong consumer cryptography because U.S. firms' dominance of the market for operating systems and other potential applications of cryptography tended to stifle the growth of indigenous competitors."[50] Now it appears that other nations may move forward with encryption standards or decide not to impose any limits, leaving the United States to play catch-up in a field it once led.[51]

C. Law Enforcement

The Clinton Administration has couched the need for limits on encryption exports in terms of security. FBI Director Louis Freeh draws a parallel between encryption exports and court-authorized wiretaps of digital telephones.[52] In 1993 when the FBI sought the assistance of Congress in maintaining and continuing court-authorized wiretaps in a new technological environment, there was no imminent crisis.[53] However, the FBI was confident that within the next decade it would lose its ability to perform such wiretaps.[54] Likewise today, the Clinton Administration does not claim that there is a crisis involving encryption.[55] Director Freeh argues that if the government waits until there is a crisis it will be too late because high level encryption will be the global standard, leaving law enforcement and national security at risk.[56]

D. Privacy Concerns

Privacy advocates are skeptical of the impact government-supported key escrow will have on their personal

---

49. *See id.* (reasoning that the virtual U.S. monopoly of the industry coupled with its export controls effectively set the foreign countries import standards at the same level).

50. *Id.*

51. *See* EXPORT STUDY, *supra* note 1, at ES-2 to ES-3.

52. *See* Louis J. Freeh, Speech by Louis J. Freeh, Director of the FBI, Remarks at the 1997 International Computer Crime Conference (Mar. 4, 1997) (transcript available at the office of the *Houston Journal of International Law*).

53. *See id.*

54. *See id.*

55. *See id.*

56. *See id.*

privacy.[57] This skepticism is heightened by the government requirement of a third party escrow holder and participation in key management.[58]

Other concerns include whether notice will be given to the encryption user when the government attains access; who will have access to the key; the type of escrowed-encryption method established as standard; the treatment of foreign governments; the treatment of foreign users versus domestic users; and the rules governing intelligence agencies.[59] Constitutional questions of privacy have also been raised,[60] but have not been prominent in the debate.

E. Freedom of Speech

The First Amendment protects speech from unconstitutional prior restraint by the government.[61] The two federal district courts that have considered the impact of export regulations on free speech have grappled with several questions. Is computer source code speech? If it is speech, is it protected? If it is protected speech, are the export limitations an unconstitutional prior restraint? [62] One of these courts found source code to be protected speech and held the regulations to be unconstitutional.[63]

---

57. *See SAFE Hearings*, *supra* note 31, at 83 (statement of Jerry Berman, Executive Director, Center for Democracy and Technology). Berman argued that government access raises several privacy questions under the Fourth and Fifth Amendments. *See id.* These questions include what legal standard to apply when domestic law enforcement seeks access; whether a court order will be required or merely the approval of a judge; whether different rules will govern intelligence agencies; and whether there should be different standards for targets that are U.S. citizens, foreign governments, or foreign citizens. *See id.*

58. *See id.* at 86 (observing that law enforcement could force users to "lodge their keys with recovery agents").

59. *See id.* at 83.

60. *See, e.g.,* Megan Connor Bertron, Note, *Home Is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 164 (1996) (comparing privacy expectations of computer users to those of telephone communications users and postal system users).

61. *See* U.S. CONST. amend. I.

62. *Compare* Thinh Nguyen, Note, *Cryptography, Export Controls, and the First Amendment in* Bernstein v. United States Dep't of State, 10 HARV. J.L. & TECH. 667, 675–76 (1997) (arguing that source code is conduct not speech), *with* Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1287 (N.D. Cal. 1996) (holding that source code is protected speech).

63. *See id.; see also* Karn v. United States Dep't of State, 925 F. Supp. 1, 9 (D.D.C. 1996) (assuming that the protection of the First Amendment extends to the source code but declining to rule whether source codes, without the comments, fall within the protection of the First Amendment).

IV. STATUS OF ENCRYPTION EXPORT REGULATIONS IN THE UNITED STATES

The Clinton Administration proposed export regulations that were in force while public comment was being taken.[64] Some within the encryption industry believe they can still be competitive in the international marketplace with the Clinton Administration's regulatory guidelines.[65] Others are pushing hard for suspension of all export regulations or are advocating for greatly diminishing them.[66] Opponents of the Clinton Administration's proposed regulations have taken their battle to Congress and to the courtroom. This Section examines the old and the new export regulations, the debate in Congress on whether changes should be made to export policy, and the legal challenges to the regulations making their way through federal courts.

A. The Clinton Administration's Export Regulations

1. Out with the Old Regulations

On December 30, 1996, the Clinton Administration published a rule transferring the licensing of commercial encryption products from the Department of State to the Department of Commerce.[67] The responsibility for regulating the export[68] of encryption technology is divided between the

---

64. *See* Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,573 (1996).

65. As of September 1997, the Department of Commerce had received over 1000 applications for encryption exports and 37 key management plans to build and market key management products. *See SAFE Hearings*, *supra* note 31, at 52 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce).

66. *See* Elizabeth Corcoran, *Microsoft's Bill, on Capitol Hill*, WASH. POST, June 5, 1997, at D3.

67. *See* Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572 (1996). These regulations are referred to as the 1997–1998 regulations to distinguish them from the 1999–2000 regulations.

68. The term "export," as defined by the Department of State in its International Traffic in Arms Regulations, includes:

> (1) Sending or taking a defense article out of the United States in any manner, except by mere travel outside the United States by a person whose personal knowledge includes technical data; or
>
> . . .

Department of State[69] and the Department of Commerce.[70] The 1996 regulations were a limited, two year liberalization.[71]

Prior to December 31, 1996 the State Department regulated the export of defense related encryption technology.[72] The Department of Commerce regulated the export of encryption technology with both civilian and military applications;[73] and also regulated encryption technology when the State Department waived its jurisdiction.[74] Under the authority of the Arms Export Control Act[75] and the International Traffic in Arms Regulations (ITAR),[76] the State Department was charged with regulating the export of defense articles, technology, and services;[77] the State Department required a license for each export.[78]

In practice, the State Department deferred to the NSA "to determine what products are subject to a licensing requirement and the licensing policy for such items."[79] The NSA is responsible for monitoring and deciphering communications abroad.[80] To fulfill this responsibility, the

---

> (3) Disclosing . . . or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government . . .; or
>
> (4) Disclosing . . . or transferring technical data to a foreign person, whether in the United States or abroad; or
>
> (5) Performing a defense service . . . for . . . a foreign person, whether in the United States or abroad.

International Traffic in Arms Regulations (ITAR), 22 C.F.R. § 120.17 (1996).

69. *See* International Traffic in Arms Regulations, 22 C.F.R. § 120.1 (1998).

70. *See id.* § 120.5 (noting that the Department of Commerce "regulates the export of items on the Commerce Control List").

71. *See* 61 Fed. Reg. 68,572, 68,573 (1996).

72. *See* 22 C.F.R. § 120.1(a) (1998) (stating that the purpose of the ITAR is "to control the export and import of defense articles and defense services").

73. *See* James B. Altman & William McGlone, *Demystifying U.S. Encryption Export Controls*, 46 AM. U. L. REV. 493, 498 (1996) (outlining the breakdown of agency jurisdiction).

74. *See* International Traffic in Arms Regulations, 22 C.F.R. § 121.1 cat. XIII(b)(1)(i)–(ix) (1996) (excepting enumerated "cryptographic equipment and software" from ITAR).

75. *See* 22 U.S.C. § 2778 (1994).

76. *See* 22 C.F.R. pt. 120 (1996).

77. *See* Altman & McGlone, *supra* note 73, at 498.

78. *See* 22 C.F.R. § 123.1 (1996).

79. Altman & McGlone, *supra* note 73, at 499.

80. *See id.*

NSA must be able to decode encrypted messages.[81] Through the control of exports, the NSA attempted to limit the level of encryption technology deployed overseas ensuring that it would be able to monitor communications abroad.[82]

2. In with the 1997–1998 Regulations

The 1997–1998 procedures were intended to promote the development of a "key management infrastructure."[83] In November 1996 President Clinton signed an executive order transferring jurisdiction for export control of commercial encryption from the State Department to the Commerce Department.[84] Under the 1997–1998 regulations, commercial encryption products had to receive an export license or qualify for a license exemption.[85]

a. License Exemption

The cornerstone of the 1997–1998 procedures was the creation of a license exemption for software and equipment that includes key management.[86] Encryption products receiving the exemption were exported freely after a review by the Departments of Commerce, Justice,[87] and Defense.[88] This

---

81. *See id.*

82. *See id.*

83. *SAFE Hearings*, *supra* note 31, at 55 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce).

84. *See* Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996).

85. *See* Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,573 (1996).

86. *See SAFE Hearings*, *supra* note 31, at 55 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce).

87. Since the transfer of jurisdiction, the FBI, part of the Department of Justice, has become more active in licensing decisions, supplanting the deference once shown to the National Security Agency (NSA). *See* Stewart A. Baker & Michael D. Hintze, *Government Regulation of Encryption: Domestic and International Developments, in* DOING BUSINESS ON THE INTERNET: THE LAW OF ELECTRONIC COMMERCE 291, 294 (PLI Patents, Copyrights, Trademarks & Literary Property Course Handbook Series No. G-4024, 1997). The Justice Department's involvement has been controversial. *See* Altman & McGlone, *supra* note 73, at 502–03. The regulations are supposed to be only concerned with export licenses, which are not within the primary expertise of the Justice Department. *See id.* (noting that this was the first time the Justice Department and FBI have participated in export licensing decisions). The Justice Department's involvement lends credence to those who suspect that the Clinton Administration is considering regulating the domestic market.

88. *See id.*

exemption was available to technology of any strength and any key length.[89]

The 1997–1998 license exemption regulations were criticized as overly strict.[90] For example, the key management agent was required to provide the Bureau of Export Administration (BXA) "detailed and specific information on the company" and on each "individual [who was] directly involved in the escrow of keys . . . ."[91] Another concern was that the procedures for the escrow agent could be read as requiring continuing monitoring,[92] which would chill customer enthusiasm for the product and would be "beyond the ability of most exporters."[93]

The 1997–1998 procedures also provided for self-escrow and escrow of keys overseas.[94] This was intended to make key recovery products more attractive to foreign markets.[95] To allay industry fears that it would take too long to obtain necessary agreements with foreign governments concerning access to the keys, the new procedures allowed the issuance of a license exemption prior to the approval by these agreements.[96]

b. Licensing Schemes

Encryption items are governed by their own category of controls and are divided into several subcategories, each of which has its own licensing scheme.[97] Under the 1997–1998 regulations, encryption technology that did not exceed 56 bit DES (Data Encryption Standard) was governed by the two-

---

89. *See SAFE Hearings*, *supra* note 31, at 55 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce). As of September 1997, three of the eight companies that had submitted requests had been approved for the license exemption. *See id.* at 56.

90. *See* Baker & Hintze, *supra* note 87, at 294.

91. *Id.*

92. *See id.* (noting the "obligation on the exporter to monitor approved key recovery agents").

93. *Id.* at 294–95.

94. *See SAFE Hearings*, *supra* note 31, at 55 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce).

95. *See Id.*

96. *See id.*

97. *See* Baker & Hintze, *supra* note 87, at 294 (citing 15 C.F.R. § 742.15(b) (1997)).

year liberalization period of the new procedures.[98] During this period, companies could export 56 bit DES if they submitted plans that demonstrated the companies' commitment to build and market key management periods.[99] Non-recovery encryption of forty bits or less were eligible for release from normal encryption item (EI) controls after a one-time review.[100]

Industry responded to these regulations in several ways. Some companies banned together to form the Alliance, an affiliation of over sixty-five international companies that joined together to facilitate the worldwide use of strong encryption through the development of key recovery.[101] The Alliance includes among its goals the definition of commercial infrastructure, the promotion of interoperability between technology using different key recovery and non-key recovery, and the evaluation of technologies to meet the changing commercial needs.[102] The Alliance does not support one form of key recovery,[103] but supports the technology and infrastructure that makes key recovery possible.[104]

IBM, a founding Alliance member,[105] has implemented its key recovery system, IBM SecureWay Key Recovery (SKR).[106] Under SKR, "no party actually holds the cryptographic key or parts of the key."[107] The key is encapsulated by key recovery fields that are "mathematically related to but not actually the key or parts of the key."[108] IBM uses the analogy of one's house key being kept by a neighbor to explain its key

---

98. *See id.; see also SAFE Hearings*, *supra* note 31, at 55 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce) (explaining the liberalization period).

99. *See SAFE Hearings*, *supra* note 31, at 55 (statement of William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Dep't of Commerce). As of September 1997, 37 companies had submitted plans for review and 32 had been approved. *See id.* at 56.

100. *See* Baker & Hintze, *supra* note 87, at 295.

101. *See High-Tech Readers*, *supra* note 28.

102. *See* Jim Lardear, *Alliance's Goal: Secure E-Commerce; Key Recovery Alliance,* MIDRANGE SYS., Feb. 14, 1997, at 37.

103. *See* International. Bus. Mach., *IBM KeyWorks and the IBM Key Recovery Technology* (visited Feb. 23, 1999) <http://www.ibm.com/security/html/wp_keymgt3.html> [hereinafter *IBM KeyWorks*] (criticizing key escrow).

104. *See* Lardear, *supra* note 102, at 37.

105. *See High-Tech Readers*, *supra* note 28.

106. *See id.*

107. *IBM KeyWorks*, *supra* note 103.

108. *Id.*

recovery technique.[109] With IBM key recovery, the homeowner does not give the key to his neighbor to hold.[110] The homeowner keeps the key in a lock box.[111] He then gives several of his neighbors one number from the combination to the lockbox.[112] All of the neighbors have to get together to open the box and even then they do not know in what order to put the numbers.[113] Variations include giving out all but one of the numbers or giving each neighbor several digits in random order.[114] Of course the homeowner need not share his key with someone outside the house.[115] Instead of neighbors, members of his household could replace neighbors in the scenario.[116] SKR has many advantages.[117] No one other than the key owner has a copy of the key or any part of the key.[118] There is no single point of vulnerability, because there are several neighbors.[119] The user need not communicate with an escrow agent each session.[120] Control of key management is not lost to a third party and "there is no need for a key storage infrastructure."[121]

As an alternative to key recovery, a company can try to get around the regulations altogether. That is what Sun

---

109. *See id.* (explaining the difference between the IBM key recovery method and key escrow).

110. *See id.*

111. *See id.*

112. *See id.*

113. *See id.*

114. *See id.*

115. *See id.* (analogizing key escrow to entrusting a house key with a friend, neighbor, or only family members).

116. *See id.*

117. *See id.*

118. *See id.*

119. *See id.*

> Consider the scenario of a lock box containing the actual house key. Suppose this lock box had a combination lock on it, and each number in the combination is given to a different party. All of the parties would have to get together and then determine the order of the digits to open the lock box and obtain the key. None of the parties have a copy of the actual key.

Id.

120. *See id.*

121. *Id.*

Microsystems did.[122] Sun Microsystems provides 128 bit and triple DES encryption over the Internet.[123] Under the 1997–1998 regulations, it was "illegal for a US company to export encryption software that exceeds 56-bit encoding. But it [was] legal to import such technology from abroad, presuming the domestic vendor had no role in its development."[124] Sun Microsystems imports encryption software from Russia that it then sells through Sun channels under the name PC SunScreen SKIP E+.[125]

c. In with the 1999–2000 regulations

On December 31, 1998, the Clinton Administration released its revised encryption regulations,[126] which addressed a number of the concerns raised about the 1997–1998 regulations. The regulations make four significant changes to the old regulations.[127] First, the latest regulations allow fifty-six bit encryption products without key recovery after a one-time review.[128] There is one limitation. As with all encryption products, non-recoverable encryption products may not be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria.[129]

Second, the Clinton Administration loosened the requirements for encryption products stronger than fifty-six bit that contain key recovery. The new regulations eliminate the previously required key recovery commitment plans, the six-month progress reports, and the prior reporting of key recovery agent information,[130] which concerned exporters.[131]

Third, the new regulations permit exports of "recoverable products" to foreign commercial firms for internal company

---

122. *See Sun Microsystems Taking on Feds Over Current US Encryption Regulations*, FED. COMPUTER MKT. REP., May 26, 1997, *available in* 1997 WL 8634876.

123. *See id.*

124. *Id.*

125. *See id.*

126. *See* Encryption Items, 63 Fed. Reg. 72,156 (1998).

127. *See id.* at 72,157 (explaining the new regulations).

128. *See id.* at 72,160.

129. *See id.* at 72,157.

130. *See id.* at 72,159 (eliminating these requirements); *see also id.* at 72,156 (explaining the changes made to the previous regulations).

131. *See* Baker & Hintze, *supra* note 87, at 294–95.

proprietary use in select countries.[132] Recoverable products allow either a recovery feature or network administrator to recover a plain text of the encrypted information without the knowledge or help of the end user.[133]

Finally, the Clinton Administration also loosened restrictions by allowing certain U.S. subsidiaries, insurance companies, companies in the health and medical sector, and on-line merchants to use unlimited encryption.[134] Allowing U.S. subsidiaries to use unlimited encryption with or without key recovery addresses the fears of business that seek to protect their corporate secrets. Likewise, allowing on-line merchants unlimited encryption regardless of key recovery addresses any concerns that the Clinton Administration's regulations were stymieing the growth of Internet commerce. Some proponents of strong encryption see the new regulations as a step by the Clinton Administration toward dropping key recovery altogether.[135]

B. Legislative Past and Present

A fierce battle over encryption export technology continues to be fought in Congress where opponents and proponents of key recovery have been the most outspoken. Obtaining passage of legislation to repeal or modify the export regulations is the best opportunity for the opponents

---

132. *See* Encryption Items, 63 Fed. Reg. at 72,164. The countries are divided into two groups. *See id.* at 72,162. Commercial entities in the first group and their branches located in either the first or second groups may "receive 'recoverable' encryption commodities and software of any key length for internal company proprietary use." *Id.* Commercial entities in the second group and their branches may "receive 'recoverable' encryption commodities and software of any key length for internal company proprietary use," as long as the branches are not located in Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. *Id.* The first group includes Anguilla, Antigua, Argentina, Aruba, Bahamas, Barbados, Brazil, Czech Republic, Dominica, Ecuador, Greece, Hungary, Kenya, Monaco, Poland, St. Kitts & Nevis, St. Vincent/Grenadines, Seychelles, Trinidad & Tobago, Turkey, Uruguay. *See id.* The second group includes Austria, Australia, Belgium, Canada, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Luxembourg, The Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, United Kingdom, and United States. *See id.*

133. *See id.* at 72,166.

134. *See id.* at 72,159–72,161.

135. *See* Rutrell Yasin, *Relenting on Encryption,* INTERNETWEEK, Sept. 21, 1998, *available in* 1998 WL 13335759 (quoting Glen Gramling, marketing manager for Hewlett-Packard's VerSecure product line, who called the regulations "an evolutionary step forward" that "will help a number of industries").

to repeal or modify the export regulation.[136] The supporters of the current regulations seem to understand that the real power is not in passing legislation, but in keeping legislation from being passed.[137]

As will be discussed, in the last Congress the bill that gained favorable consideration in the Senate bore little resemblance to legislation considered by the House of Representatives. The House of Representatives tried to pass a compromise bill that could then be considered by the Senate. The passage of this bill was complicated by the fact that each of the committees with appropriate jurisdiction in the House of Representatives passed its own version of the bill. It appears unlikely that Congress will resolve these conflicts and pass any meaningful encryption export legislation in the near future because neither of the bills favored by each chamber could garner enough support to pass in the last session, and neither bill much resembled the other.[138]

1. The Senate

During the 105th Congress, the Secure Public Networks Act (Senate Bill 909)[139] was the only export reform legislation to receive any favorable consideration by the Senate.[140] It was the only measure in Congress to have the support of the Clinton Administration.[141] This bill gave "the Secretary of Commerce . . . jurisdiction over the export of commercial encryption products [and] the sole duty to issue export licenses on . . . products."[142] Encryption products up to and including 56 bit DES were exempted after a one-time review regardless of whether the products contain key recovery.[143]

---

136. *See* Interview with Patrick Woerhle, Legislative Assistant to Congressman Ken Bentsen, in Houston, Tex. (Jan. 27, 1998).

137. *See id.*

138. *Compare* S. 909, 105th Cong. (1997), *with* H.R. 695, 105th Cong. (1997).

139. *See* S. 909, 105th Cong. § 1 (1997).

140. *See* NUNNO, *supra* note 17, at 7–12. The Senate Commerce Committee approved the measure. *See id.* at 7–12. However, it did not file its report. *See id.* The Senate Judiciary Committee held a hearing on July 9, 1997 at which the bill was discussed. *See id.* at 11. FBI Director Louis Freeh objected to the fact that key recovery is not required under the bill. *See id.* He feels key recovery should be mandatory to enable monitoring of criminals and terrorists. *See. id.*

141. *See id.* at 7–8, 11.

142. S. 909 § 301.

143. *See id.* § 302. This would be a significant increase over the current exemption of 40 bit DES. *See* Baker & Hinze, *supra* note 87, at 295.

Senate Bill 909 would have given the President the authority to increase the strength of the export standard of encryption products without further Congressional action.[144] It also prohibited export of any encryption product if the Secretary found that a product "would be used in acts against the national security, the public safety, transportation systems, communications networks, financial institutions or other essential systems of interstate commerce; diverted to a military, terrorist or criminal use; or re-exported without authorization."[145] Finally, the bill required that the following be based on a qualified system of key management: any encryption products purchased with federal funds or otherwise procured by the U.S. government and any communications network established by the United States which uses encryption products.[146] The motivation behind this provision was to encourage key management as the standard norm in encryption products.[147] The reasoning behind this was that because the federal government and those who receive federal funds comprise a significant portion of encryption consumers, industry will opt to include key management in all of its software rather than market two domestic versions.[148]

A second Senate Bill that received favorable press among privacy advocates and opponents to government regulation of encryption exports is the Promotion of Commerce On-Line in the Digital Era Act of 1997,[149] also known as the Pro-CODE bill (Senate Bill 377).[150] The Pro-CODE bill mandated that the Commerce Department require only a general license for any computer software that is generally available or available in the public domain.[151] Pro-CODE contained provisions similar to Senate Bill 909 concerning public safety.[152] Pro-CODE also required the manufacturer or publisher of encryption software or hardware to report to the Secretary of Commerce

---

144. *See* S. 909 § 303.

145. *Id.* § 306.

146. *See id.* §§ 202–04

147. *See* Frank L. Dixon, *Encryption on the Net,* WASH. POST, Aug. 19, 1996, at A14.

148. *See id.*

149. *See* S. 377, 105th Cong. § 1 (1997).

150. *See id.*

151. *See id.* § 5(c)(2)(A).

152. *See id.* § 5(c)(3)(B).

the same information that is currently required.[153] However, under Pro-CODE the information would have been required within thirty days after the export and not as a contingency of export as required by the 1996 regulations.[154] The bill also gave the Department of Commerce exclusive domain over commercial encryption exports.[155] Pro-CODE was offered as an amendment to Senate Bill 909 during markup of that bill by the Commerce Committee.[156] The amendment was defeated eight to twelve.[157]

2. The House of Representatives

During the 105th Congress, the House of Representatives considered its own reforms of encryption export regulations. Five versions of House Bill 695, Security and Freedom through Encryption (SAFE) were considered in the House of Representatives.[158] All five versions contained significant variations from the original. The original version of SAFE codified existing domestic use policy, which had no limitation on encryption strength and no requirement for key recovery.[159] The bill also made it lawful for any person to sell encryption without key recovery and prohibited any requirement that would make a person in lawful possession of a key relinquish it to anyone except for law enforcement personnel acting under the law.[160] The original bill also made it illegal to use encryption in furtherance of a crime.[161] Section 3 gave the Secretary of Commerce exclusive authority over export of all computer hardware, software, and security technology, including encryption.[162] This section also allowed "generally available" commercial encryption to be exported without a license.[163]

---

153. *See id.* § 5(c)(4)(A).

154. *See id.* § 5(c)(4)(A)–(B).

155. *See id.* § 5(c)(1).

156. *See* NUNNO, *supra* note 17, at 10.

157. *See id.*

158. *See* H.R. 695, 105th Cong. (1997). The bill was referred to five committees, each of which reported its own version. *See* H.R. REP. NO. 105-108, pts. 1–5 (1997).

159. *See* H.R. 695 § 2, at 4–7 (referring to the originally proposed text); *see also* NUNNO, *supra* note 17, at 8.

160. *See id.* H.R. 695 § 2 at 4–7.

161. *See id.* § 3, at 7–12.

162. *See id.* An exception is technology for military use. *See id.*

163. *See id.*

The remainder of this section provides a brief synopsis of the SAFE bill passed by the following: Commerce Committee, the Intelligence Committee, the National Security Committee, the Judiciary Committee, and the International Relations Committee.

a. Commerce Committee Version

The Commerce Committee version of SAFE was identical to the original measure in several ways. It, too, prohibited mandatory use of key management, gave the Secretary of Commerce exclusive jurisdiction over export of commercial encryption, and prohibited export controls on generally available commercial encryption except for military end-uses or to certain individuals or organizations in specific foreign countries.[164] However, the bill was amended in committee to include the creation of a federal clearinghouse to assist law enforcement in decrypting electronic messages and to incorporate Section 203 of House Bill 1964.[165] The Commerce Committee defeated an amendment that would have imposed domestic use restrictions.[166]

b. Intelligence Committee Version

The House Committee on Intelligence substantially revised the bill. The Intelligence Committee version replaced the bill's original procedures that liberalized exports with procedures similar to the current regulations that restrict exports.[167] The Intelligence version would have curbed the

---

164. *See id.* §§ 2–3, at 91–107 (version passed by Commerce Committee).

165. *See id.* § 2, at 91–101. Section 203 was offered as an amendment to H.R. 695 by Representative Markey and accepted by the Committee. *See* NUNNO, *supra* note 17, at 9, 13. The amendment comes from Section 203 of Representative Markey's own encryption export bill, H.R. 1964, the Communications Privacy and Consumer Empowerment Act. *See id.* Section 203 of the bill would codify the existing domestic use policy, and eliminate the government requirement of key escrow as a contingency for licensing or regulatory approval or as a contingency to the issuance of certificates of authentication or of authority. *See id.*

166. *See id.* at 9.

167. *See* H.R. 695, at 37–90 (version passed by Intelligence Committee). This bill set a deadline of January 31, 2000 for the export of encryption products regardless of strength to be exported if they are submitted for a one-time review, do not fall under some other license requirement, and include features that provide immediate access to plain text data or decryption information from the encryption provider. *See id.* § 302, at 76–79; *see also* NUNNO, *supra* note 17, at 9.

sale of unrestricted encryption within the United States.[168] President Clinton indicated that he did not support a limit on domestic sales of encryption technology; therefore, the Intelligence Committee may have gone further than the President would support.[169]

c. National Security Committee Version

The National Security Committee supported a version that would have allowed the President to set the maximum level of encryption strength that could be exported after a one-time review.[170] It also gave joint jurisdiction over encryption exports not on the munitions list to both the secretaries of Commerce and Defense.[171]

d. Judiciary Committee Version

The Judiciary Committee version of SAFE added members of the intelligence community to the provision allowing law enforcement officers access to an encryption key if acting under law.[172] The Judiciary Committee version also clarified the section on the unlawful use of encryption in furtherance of a criminal act. This version of the bill required that the encryption be done "knowingly and willfully" in furtherance of a felony with the intent to avoid detection.[173] The committee also authorized the Attorney General to collect data on instances where encryption has "interfered with, impeded, or obstructed the ability of the Department of Justice to enforce the criminal laws of the United States."[174]

e. International Relations Committee Version

The International Relations Committee version substantially revised the original Section 3 governing exports

---

168. *See* H.R. 695 § 104, at 49–53 (proposed section 2804); *See also* NUNNO, *supra* note 17, at 9 (observing the requirements placed on encryption products that would be manufactured and distributed in the United States).

169. *See* NUNNO, *supra* note 17, at 4.

170. *See* H.R. 695 § 3, at 12–15; *see also* NUNNO, *supra* note 17, at 9.

171. *See* H.R. 695 § 3(a), at 12–13; *see also* NUNNO, *supra* note 17, at 9.

172. *See* H.R. 695 § 2, at 17–18 (proposed subsection 2804); *see also* NUNNO, *supra* note 17, at 8.

173. *See* H.R. 695 § 2, at 18–19 (proposed subsection 2805).

174. H.R. 695 § 4, at 24. The Commerce Committee included an identical provision when it considered the bill four months later. *See* H.R. 695 § 5, at 111-12.

of encryption.[175] The committee supported allowing encryption software that is generally available or in the public domain to be exported without a license.[176] The committee defeated an "amendment . . . that would have allowed the President to deny export licenses for national security reasons (including 'the ability of law enforcement agencies . . . to combat espionage, terrorism, illicit drugs, kidnapping, or other criminal acts, or otherwise would involve the potential for loss of human life.')."[177] The International Relations Committee version includes a section supporting international cooperation.[178]

3. Congressional Stalemate

The House Rules Committee did not consider any of the versions of House Bill 695 for further action in the 105th Congress.[179] It appears uncertain whether the opponents of the Clinton Administration's regulations will obtain legislative relief in the foreseeable future. However, supporters of House Bill 695 are encouraged that legislation could be accomplished this year.[180] That optimism is fueled by the large number of original co-sponsors of the legislation, the support the bill has received from industry, privacy, and consumer groups, the retirement of legislators who opposed House Bill 695, and the fact that legislators are better educated about the issue this session.[181]

Complicating any best case scenario for critics of the Clinton Administration's policy were the significant differences between the multiple versions of House Bill 695 and Senate Bill 909, the only bill to have received any favorable consideration in the Senate.[182] Opponents to encryption export regulations have already proposed legislation in the next Congress.

---

175. *Compare* H.R. 695 § 3, at 7–12 (original version), *with* H.R. 695 § 3, at 28–36 (version passed by the International Relations Committee).

176. *See id.* § 3, at 28–36.

177. NUNNO, *supra* note 17, at 9.

178. *See* H.R. 695 § 4, at 36–37.

179. *See* NUNNO, *supra* note 17, at 8.

180. *See* Rutrell Yasin, *Crypto Export Reform Could be Close at Hand*, INTERNETWEEK, March 15, 1999, *available in* 1999 WL 8430105. House Bill 850 had 205 bipartisan co-sponsors when it was introduced. *See id.* House Bill 695 had 55 original co-sponsors. *See id.*

181. *See id.*

182. *See* discussion *supra* Part IV.B.2.

Congressman Bob Goodlatte reintroduced a new version of the SAFE Act (House Bill 850) for consideration in the 106th Congress.[183] In what may be a sign that the Republican House majority would like to deal with this issue swiftly, the bill was referred only to the Judiciary Committee and the International Relations Committee.[184] In addition, it was voted out of the Judiciary Committee on March 24, 1999, one month after it was referred.[185]

As filed, the bill contains substantial differences from the version considered by the previous Congress.[186] The most controversial change is the addition of language that makes it a crime to conceal either incriminating communications or information relating to a felony for the purpose of avoiding detection.[187] In addition, House Bill 850 prohibits the use of encryption from being "the sole basis for establishing probable cause with respect to a criminal offense or a search warrant."[188]

C. Judiciary

The encryption export licensing requirements have been challenged in three cases,[189] two of which are examined here: *Bernstein v. United States Department of State*[190] and *Karn v. United States Department of State*.[191] The *Bernstein* court held in favor of those against limits on encryption exports.[192] Daniel Bernstein, a graduate student at the University of California at Berkeley, challenged a ruling by the NSA denying him a license to publish a new encryption algorithm electronically.[193] In December of 1996, the court ruled that

---

183. *See* Security and Freedom through Encryption (SAFE) Act, H.R. 850, 106th Cong. (1999).

184. *See id.*

185. *See Bill Tracking Report* HR 850, Bill Tracking Report (Congressional Info. Serv.) (April 7, 1999), *available in* LEXIS, Codes Library, Bltrck File.

186. *Compare* H.R. 850, *with* H.R. 695, 105th Cong. (1997).

187. *See* H.R. 850 § 2, at 7 (proposed subsection 2805(a)). The bill requires an intent to conceal. *See id.*

188. *See id.* § 2, at 7 (proposed subsection 2805(b)).

189. A third case, *Junger v. Daley*, found encryption source code not to be protected speech, because it is "exported to transfer functions, not to communicate ideas." *See* 8 F. Supp. 2d 708, 716 (D. Ohio 1998).

190. 922 F. Supp. 1426 (N.D. Cal. 1996).

191. 925 F. Supp. 1 (D.D.C. 1996).

192. The Court held the rules to be unconstitutional. *See* Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1288 (N.D. Cal. 1996).

193. *See* Bernstein, 922 F. Supp. at 1428–30.

encryption source code is speech protected by the First Amendment and that the pre-1996 regulations are an unconstitutional prior restraint on free speech.[194] Following the promulgation of the 1996 regulations, the court declared that the Commerce Department regulations requiring licenses for encryption exports also amount to an unlawful prior restraint on First Amendment activity and as such are unconstitutional.[195] The Ninth Circuit Court of Appeals recently upheld the lower court's decision, but on narrower grounds.[196]

The *Karn* case has been more favorable to the Clinton Administration and proponents of limits on encryption exports.[197] Philip Karn, a U.S. engineer, sought permission from the State Department to export the text of a book about encryption in floppy disk form.[198] The book provided program language for a version of cryptographic software.[199] The State Department's Office of Defense Trade Controls determined that the diskette was subject to ITAR control, and Karn appealed.[200] His appeal was denied and Karn filed suit.[201] The court granted the government's request for summary judgment, holding that the State Department's export licensing process was not subject to judicial review.[202] The court held that regulation of encryption software does not amount to restraint of free speech[203] and declined to rule on whether the program language of encryption software fell within the protection of the First Amendment as speech.[204] Upon appeal by Karn, the appellate court remanded the case to determine if any alternative grounds for resolution existed

---

194. *See* Bernstein, 945 F. Supp. at 1288.

195. *See* Bernstein v. United States Dep't of State, 974 F. Supp. 1288, 1308 (N.D. Cal. 1997).

196. *See* Bernstein v. United States Dep't of State, No. 97-16686, 1999 U.S. App. LEXIS 8595, at *3 (9th Cir. May 6, 1999).

197. *See Karn*, 925 F. Supp. at 11 (stating that the "court will not scrutinize the President's foreign policy decision" as it pertains to cryptographic product on ITAR).

198. *See id.* at 2–4.

199. *See id.* at 4.

200. *See id.*

201. *See id.*

202. *See id.* at 8, 14.

203. *See id.* at 12, 13.

204. *See id.* at 9, n.19.

as is necessary when answering questions involving the Constitution of the United States.[205]

In determining whether speech is protected from export controls, "courts must balance First Amendment protections with the government's regulation of export privileges."[206] When applying this standard, "[c]ourts consistently have upheld national security-based restrictions on exports of information."[207] "That is, in determining the constitutionality of encryption export controls, courts must ascertain whether there is a sufficiently compelling governmental interest in regulating encryption exports and whether the regulation is narrowly tailored to further that interest."[208] Content-neutral regulation may be justified as long as the regulation "'furthers an important or substantial governmental interest,' and 'the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.'"[209]

The rulings have had little impact to date. The district court limited its *Bernstein* ruling to that particular plaintiff and the *Karn* case was sent back to the district court for reconsideration. However, the Ninth Circuit's opinion could have widespread implications unless it is stayed.[210] It will probably take several years for either case to make its way through the judicial process to a point where it will have widespread impact, if any at all.

V. INTERNATIONAL PERSPECTIVE ON REGULATION

Regulations passed by other nations have a profound impact on the U.S. encryption industry's ability to participate in foreign markets.[211] Foreign domestic regulations control what kind of encryption, if any, can be imported by foreign domestic users.[212] Foreign export regulations control what

---

205. *See* Karn v. United States Dep't of State, No. 96-5121, 1997 WL 71750, at *1 (D.C. Cir. Jan. 21, 1997) (per curiam).

206. Altman & McGlone, *supra* note 73, at 508–09.

207. *Id.* at 508.

208. *Id.* at 509.

209. *Karn*, 925 F. Supp. at 1, 11 (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

210. *See* Declan McCullagh, *Landmark Ruling on Encryption*, (May 6, 1999) <http://www.wired.com/news/news/politics/story/19553.html> (noting that unless the decision is stayed it will be legal to post source code on the Internet in California, Washington, and Oregon).

211. *See* CRISIS STUDY, *supra* note 5, at 430–31.

212. *See id.* at 437 (observing for example, "buy American" laws).

products are available to compete in the U.S. market and also serve to support or undermine attempts by the U.S. government to regulate U.S. exports.[213]

When a nation regulates its domestic use, foreign industry has to meet those regulations in order to compete in the regulated markets.[214] Import controls and use controls[215] are available to nations to restrict domestic use of cryptography. These controls may take the form of explicit law or decree (which may or may not be consistently enforced), of informal control, or of a variety of other mechanisms including laws relating to public telephone systems, to the content carried by electronic media, or to licensing arrangements.[216] Because the United States is currently the largest exporter of computer software and potentially a large exporter of encryption technology, these regulations will have a significant impact on U.S. industry.[217]

This section will attempt to answer several questions for each international governing body discussed below. To what extent has the international governing body regulated domestic use of encryption technology? To what extent has the nation regulated export of encryption technology. If it has regulated the market or is considering doing so, will these regulations be market or government driven? Do regulatory proposals provide for market encryption? If so, who will hold the keys and under what circumstances does the key holder release the keys to other parties?[218] This section will close on how nations can reach consensus on international cryptography policy regarding exports and use.[219]

---

213. *See id.* at 431.

214. *See* Baker & Hintze, *supra* note 87, at 303–05 (detailing regulatory requirements of foreign governments).

215. *See* CRISIS STUDY, *supra* note 5, at 436 (defining import controls as "restrictions on products with encryption capability that may be taken into a given nation," and defining use controls as "restriction on the use of [encryption] products within [a nation's] jurisdiction").

216. *See id.* at 436–37.

217. *See id.* at 431.

218. *See id.* at 444.

219. *See id.* at 447.

A. International Governing Organizations

1. The Organisation for Economic Cooperation and Development

The Clinton Administration pushed hard for the Organisation for Economic Cooperation and Development (OECD)[220], an international organization of the industrial market-economy countries, to adopt key management.[221] On March 27, 1997, the OECD adopted cryptography guidelines.[222] Although the actual guidelines were not made public, eight general principles were released.[223] While not binding, these principles are very influential among policy

---

220. *See* Organisation for Econ. And Coop. Dev., *About OECD* (visited Feb. 8, 1999) <http://www.oecd.org/about/general/index.htm> (noting that the United States is the biggest financial contributor to the OECD).

221. *See OECD Approves Cryptography Guidelines; Rebuffs Administration's Key Recovery Plan*, Int'l Trade Daily (BNA) (March 28, 1997), *available in* LEXIS, News Library, Bnaitd File.

222. *See id.*

223. *See id.* The eight general principles are:

- Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communication systems.
- Users should have a right to choose any cryptographic method, subject to applicable law.
- Cryptographic methods should be developed in response to the needs, demands, and responsibilities of individuals, business and governments.
- Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.
- The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptographic policies and in the implementation and use of cryptographic methods.
- National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.
- Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.
- Governments should cooperate to coordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

Id.

makers.[224] The OECD sought to strike a balance between individuals' right to privacy, business concerns over technology development and commerce, and governments' demand for continuing access to encrypted material.[225] To the Clinton Administration's disappointment, the OECD did not come out with a strong position in favor of key management.[226] However, the conference was extremely important as an educational tool for the Clinton Administration.[227] Nations that had not considered key management left the conference more sympathetic to the U.S. concerns.[228]

2. European Union

On October 8, 1997, the European Union (EU) published a framework policy paper that "calls for unlimited, market-driven use of encryption technology in the European Union to enhance security and boost electronic commerce on the Internet."[229] The paper provides for the crypto key to be held by third party holders not selected by government, but by market forces.[230] The EU does not want its member countries to pass restrictive legislation.[231] However, one member country, France, has already done so and other member countries may soon do the same.[232] The EU and the United States differ on whether to regulate the domestic market versus the export market.[233] The EU wants market forces and

---

224. *See* Stewart A. Baker, *Decoding the OECD's Guidelines for Cryptography Policy*, *in* DOING BUSINESS ON THE INTERNET: THE LAW OF ELECTRONIC COMMERCE 267, 269 (PLI Patents, Copyrights, Trademarks & Literary Property Course Handbook Series No. G–491, 1997).

225. *See* Baker & Hintze, *supra* note 87, at 302 (observing the eight guidelines of the OECD).

226. *See id.* (noting there was not a mandate for the encryption policy favored by the United States).

227. *See id.*

228. *See id.*

229. *EU Dismissing US Concerns, Proposes No Limitations On Encryption Technology,* Int'l Trade Daily (BNA) (Oct. 9, 1997), *available in* LEXIS, News Library, Bnaitd File.

230. *See id.*

231. *See id.* (noting that the 15 member states have been asked to refrain from passing legislation concerning encryption until a common policy can be worked out).

232. *See id.* Other member countries considering restrictive legislation are Germany, Italy, the Netherlands, and Denmark. *See id.*

233. *See id.*

industry self-regulation for encryption; the United States does not.[234] The United States wants market forces and industry self-regulation for data protection; the EU does not.[235] The EU has proposed an international charter with the United States.[236]

3. The Wassenaar Arrangement

At its fourth Plenary meeting held December 2–3, 1998 in Vienna, Austria, the thirty-three signatories to the Wassenaar Arrangement[237] agreed in principle "to limit exports of strong encryption products."[238] This is a significant departure from "the previous version that allowed for the export of strong mass-market" encryption.[239] It remains to be seen exactly what impact the new version will have on the encryption export market as many of the details need to be worked out. However, the Clinton Administration was encouraged by the agreement. The United States, United Kingdom, France, Japan, and Russia are all members of the Wassennar Arrangement.[240]

B. Countries Who are Major International Encryption Players

1. United Kingdom

The United Kingdom is concerned with encryption policy and took a stance very similar to that of the United States throughout the OECD process,[241] but it does not currently have import controls on encryption products.[242] The United Kingdom issued a policy statement promising that it was not

---

234. *See id.*

235. *See id.*

236. *See id.*

237. *See* Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Tech., *Public Statement*, (Dec. 3, 1998) <http://www.wassenaar.org/docs/press_4.html> [hereinafter *Wassenaar Public Statement*].

238. Declan McCullagh, *Strong Rules for Strong Crypto*, (Dec. 8, 1998) <http://www.wired.com/news/news/politics/story/16693.html>.

239. James Glave, *Will Arms Treaty Hurt Privacy?,* (Dec. 4, 1998) <http://www.wired.com/news/news/technology/story/16651.html>.

240. *See Wassenaar Public Statement*, *supra* note 237.

241. *See* Baker, *supra* note 224, at 270–71 (reporting that both the United States and the United Kingdom shared a "view of cryptography that was shaped principally by the concerns of law enforcement and national security agencies").

242. *See* EXPORT STUDY, *supra* note 1, at II-31 and II-32.

the intention of the government to regulate the private use of encryption.[243] The statement supported the licensing of a Trusted Third Party (TTP)[244] so as to engender trust while balancing "commercial requirement for robust encryption services," protection of users, and the need for "intelligence and law enforcement authorities to retain the effectiveness of warranted interception."[245]

2. France

In January 1999, the Interministerial Committee on the Information Society released its decision on encryption.[246] The decision outlines legislation to be presented to Parliament by the Prime Minister.[247] The proposed legislation will allow domestic use of encryption without a mandatory key escrow provision and will allow export of encryption methods that do not exceed fifty-six bits.[248]

In 1997, France considered a draft decree that would implement encryption legislation passed in 1996 as an amendment to the Telecommunications Regulation Act.[249] Under the proposed law, individuals and entities will be prohibited from using encryption unless: "(1) the prime minister has authorized such use, or (2) the encryption keys have been deposited with a trusted third party."[250] Under the draft decree, the TTP must operate within France and be subject to prior approval by the Prime Minister.[251] Unless otherwise approved by the Prime Minister, the entity must also be: "an individual company owned by a French resident;

---

243. *See* Department of Trade and Indus., *Government Sets Out Proposals for Encryption on Public Telecommunications Networks,* (visited Feb. 1, 1999 <http://www.worldserver.pipex.com/coi/depts/GTI/coi9303b.ok> (offering provisions for the United Kingdom to utilize in safeguarding "the integrity and confidentiality of electronic information transmitted on public telecommunications networks").

244. *See id.*

245. *Id.*

246. *See* Interministerial Comm. on the Information Society (CISI), *Decisions Taken; Build a Legislative Framework to Protect Exchanges and Privacy*. (Jan. 19, 1999) <http://www.premier-mnistre.gouv.fr/gb/info/fiche1gb.htm>

247. *See id.*

248. *See id.*

249. *See Electronic Commerce: French Propose to Ban Crypto Systems Where Key is Escrowed Outside of France*, Int'l Trade Daily (BNA) (Sept. 24, 1997) *available in* LEXIS, News Library, Bnaitd File.

250. *Id.*

251. *See id.*

[a] personal [company] with French partners and managers; or [a] capital and limited liability [company] whose managers, agents, and directors of the board, the executive committee, or the supervisory committee are French."[252] The French government will not share keys that have been escrowed with another government or products with "traps" and "backdoors" that would allow persons other than French officials to access the contents of an encrypted message.[253]

3. Japan

Japan currently has no import or use restrictions on encryption.[254] Whereas in other countries multiple interests influence encryption policy, in Japan commercial interests dominate encryption policy.[255] The Japanese government differs from other countries, especially the United States, in that it does not have the power to monitor domestic communications and therefore does not feel compelled to impose limits on domestic encryption capabilities.[256] Instead, the development and export of high level encryption is seen by the Japanese as a way to penetrate the global information infrastructure.[257] The Japanese government views cryptography as a "central enabling technology for digital commerce" and has backed its commitment to encryption with substantial funding.[258] The Information-Technology Promotion Agency, an arm of the Ministry of International Trade and Industry, plans "to spend more than $300 million on research and development to evaluate cryptography for electric commerce."[259]

A prominent analyst, Stewart A. Baker, warns that unless Japanese policy alters as a result of participation in international policy discussions, Japan could pose a major challenge to U.S. escrow policy.[260] There have been some

---

252. *Id.*

253. *See id.*

254. *See* EXPORT STUDY, *supra* note 1, at II-23.

255. *See* Baker & Hintze, *supra* note 87, at 305–06.

256. *See id.* at 306 (explaining that the Japanese police face constitutional constraints regarding wiretapping).

257. *See id.* at 305.

258. *Id.* at 306.

259. *Id.*

260. *See* Stewart Baker, *Japan Enters the Crypto Wars* (visited Feb. 6, 1999) <http://www.wired.com/wired/4.09/es.crypto.html> (arguing that Japan is the player to watch in the crypto wars).

changes in Japan which may bear on its encryption policy.[261] In late 1995, the "Ministry of Justice began seeking legislation authorizing law enforcement wiretapping and bugging of criminal suspects."[262] The National Police Agency and Ministry of Justice, which have not been involved in encryption policy in the past because of the ban on monitoring domestic communications, have taken a more active role.[263] Japan now requires "prior government approval from MITI [Ministry of International Trade and Industry] for any overseas sale of encryption for more than 50,000 yen."[264] Whether this is a result of the Wassenaar Arrangement, requiring record keeping for sales greater than 50,000 yen, as MITI officials portend or the result of pressure from the United States, which has been speculated, is unclear.[265] At the OECD session in June 1996, Baker observed that by the end of discussions the Japanese delegation had been expanded to include Japanese police representatives; he also noted a marked difference in the nature of the Japanese delegation, it having taken a more low-key profile.[266]

4. Russia

Russia has not yet embraced key management. Russia is not a member of OECD, which is debating the future of encryption regulation.[267] However, it is a member of the Wassenaar Arrangement, which has also been instrumental in international debates on encryption regulation.[268] In April 1995, President Yeltsin issued a decree banning unauthorized encryption.[269] The edict bans development, import, sale, and use of unlicensed encryption devices, as

---

261. *See* Baker & Hintze, *supra* note 87, at 306.

262. *Id.*

263. *See id.*

264. *Id.*

265. *See id.*

266. *See* Baker, *supra* note 260 (referring to Japan becoming silent at the OECD after their police representative spoke).

267. *See* Organisation for Econ. And Coop. Dev., *About OECD: Membership* (visited Feb. 12, 1999) <http://www.oecd.org/general/member-countries.htm> (listing the 20 founding OECD members and the other nations who have joined since 1961).

268. *See* Baker & Hintze, *supra* note 87, at 304.

269. *See* Sobr. Zakonod. RF, 1995, No. 334, [weekly] ¶ 2; *see also* EXPORT STUDY, *supra* note 1, at II-27 (citing edict number 334 of the President of the Russian Federation).

well as protected technological means of storage, processing and transmission of information.[270]

The edict requires an exporter or importer of encryption products to obtain a license from the Ministry of Foreign Economic Relations.[271] Prior to granting the license, the Ministry consults with the Federal Agency of Government Telecommunications and Information (FAPSI).[272] To comply with the edict's controls on development, production, sales, or usage of encryption products, the products must also be certified by FAPSI.[273] In practice, this ban is not strictly enforced.[274]

5. China

China currently has no controls on encryption technology.[275] China is not part of an organization promoting a global consensus or dialog on encryption technology.[276] China has not sent representatives to major international meetings on encryption.[277] Therefore, China is considered to be the "least likely major power[] to join in an international consensus on encryption policy."[278] One noted scholar has suggested that China will not want to cooperate on a sensitive issue such as encryption because it is the frequent target of sanctions due to arms proliferation and human rights abuses.[279] In 1996, a major U.S. supplier of encryption software, RSA Data Security, Inc., took advantage of this freedom from regulation and began producing full-strength encryption software in China to export to other countries.[280]

---

270. *See* Sobr. Zakonod. RF, 1995, No. 334 [weekly] ¶¶ 2–7.

271. *See id.* ¶ 5.

272. *See id.*

273. *See id.* ¶ 2.

274. *See* Baker & Hintze, *supra* note 87, at 305.

275. *See* Altman & McGlone *supra* note 73, at 505.

276. China is not a member of the Wassenaar Arrangement or the OECD. *See* Baker & Hintze, *supra* note 87, at 305.

277. *See id.*

278. *Id.*

279. *See id.*

280. *See* Don Clark, *China, U.S. Firm Challenge U.S. On Encryption-Software Exports*, WALL ST. J., Feb. 8, 1996, at A10 (reporting the partnership formed by data encryption leader RSA Data Security and the Chinese government "that exploits loopholes in U.S. export restrictions on code-making technology").

C. Potential for International Agreement

An agreement between nations on forming an international encryption policy is difficult to imagine.[281] Some nations may agree to common policies; other nations may implement policies unique to each nation.[282] Conceptually, a global information infrastructure is adaptable to either policy structure.[283]

Significant obstacles exist to attaining an international consensus on exports and use.[284] Harmonization of export policies will have to preserve law enforcement and intelligence gathering capabilities.[285] This will require the achievement of four principles:

- Rough concurrence among nations exporting cryptography about the nations whose access to encryption capabilities should be kept to a minimum and what policy toward those nations should be;
- Willingness to allow relatively free trade in products with encryption capabilities among member nations;
- Willingness to abide by prohibitions on re-export to rogue nations; and
- Agreement among member nations about the types of encryption capabilities that would constitute a threat if widely deployed.[286]

Even if the necessary agreements are obtained, additional problems must be overcome.[287] It is not clear that developed nations have a monopoly on encryption technology given the widespread knowledge of the algorithms, and there is not a pervasive threat motivating the nations participating in the debate on whether to regulate encryption.[288] Finally, any agreement must satisfy the conflicting individual "needs of participating nations for third-party decryption before they will agree to relax import and use controls."[289] A

---

281. *See* CRISIS STUDY, *supra* note 5, at 441.

282. *See id.*

283. *See id.*

284. *See id.* at 433–34.

285. *See id.* at 447.

286. *Id.*

287. *See id.* at 448.

288. *See id.*

289. *Id.*

harmonization of policies regarding encryption use is now stymied by the inability to attain an international consensus.[290]

Any strategy by the United States to act unilaterally has been sharply criticized.[291] A unilateral strategy would incorporate some of the needs of other nations and use the dominance of the U.S. encryption community to force key management as the international standard through the use of export limits and international organizations.[292] A Congressionally mandated study rejected a unilateral strategy as a plausible option finding it to be misguided and infeasible.[293] Should such a strategy be possible, U.S. national policy would be the de facto international policy.[294] The study found that while it is an important player, the United States does not dominate international communications and information transfer.[295] Absent such power, the study held that the United States cannot operate unilaterally and must "reach accommodation with other national governments."[296]

VI. CONCLUSION

The export of encryption technology abroad is a potentially lucrative market for the U.S. encryption industry. Increased commerce conducted via the Internet may be the irreversible wave of the future. However, the need for law enforcement to access potentially life threatening information under the proper conditions is legitimate. Both law enforcement and industry advocates represent legitimate social goals. However, neither should be allowed to declare total victory at the expense of society as a whole.

Arguments that the U.S. industry will fail if encryption export regulations continue appear hollow when viewed in light of the efforts by many companies within the industry to compete within the regulations and who obviously believe they can do so successfully.

---

290. *See id.* (explaining "that the dialogue on harmonizing policies across national borders has not yet matured").

291. *See id.* at 439–40.

292. *See id.* (arguing that a de facto standard would be created).

293. *See id.* at 440.

294. *See id.*

295. *See id.*

296. *Id.*

At the end of 1998, the Clinton Administration imposed new guidelines. The Courts and congressional proposals will not answer this question in a timely manner; therefore, these guidelines do not serve as viable solutions. There is no global consensus on how to regulate the industry; and there will not be agreement for some time, as other countries struggle to determine their own encryption requirements. There is a pressing need to resolve the issue of domestic regulation in the very near future so that the U.S. encryption industry can provide greater encryption protection to an ignored domestic market. The U.S. encryption industry stands poised to lose its competitive edge in the global marketplace as a result of its own obstinacy in refusing to accept the security limitations placed on commerce and not as a result of export controls. The U.S. encryption industry needs to join forces with the Clinton Administration and find a suitable compromise on how to regulate encryption exports.

The Clinton Administration, industry, and Congressional leaders could take a few simple steps to head off this impending crisis. The parties should agree on a set of principles to govern access by law enforcement to encrypted data and to address legitimate privacy concerns. The parties should also agree on a target date by which the regulation of encryption exports will be minimized and by which key recovery products will be exported at unlimited key lengths with key recovery. Five years should allow sufficient time to formulate and implement the rules, as well as to develop and market new key escrow technology. After agreeing to a set of general principles, the parties should then use the rulemaking process to implement these principles. The rulemaking process is an opportunity for all parties to provide input for the creation of new regulations. If used correctly, it also can be much quicker than the passage of legislation. Often legislation requires implementing regulations to be promulgated before it can be enforced. This would require an unacceptable time delay. To continue to promote the development of key escrow technology during these discussions, the Clinton Administration should extend the 1996 regulations for another two year period.

Working together, the Clinton Administration, the encryption industry, and Congress can resolve their differences in a timely manner and preserve the U.S. competitive edge in this critical market.

Christina A. Cockburn†

† This comment won the Royston, Rayzor, Vickery, & Williams Writing Award. The author would like to thank Richard Savoye and Merle Morris for their guidance in writing this comment.