American University International Law Review

Volume 15 | Issue 1 Article 4

1999

The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests

Karim K. Shehadeh

THE WASSENAAR ARRANGEMENT AND ENCRYPTION EXPORTS: AN INEFFECTIVE EXPORT CONTROL REGIME THAT COMPROMISES UNITED STATES' ECONOMIC INTERESTS

KARIM K. SHEHADEH*

* J.D. Candidate, May 2001, American University Washington College of Law; B.A., Politics, 1994, Ithaca College. Special thanks to my parents, Kamal and Adonis Shehadeh, and my brother, Fady, for all of their encouragement and support throughout this process. In addition, I would like to thank my classmates and the editorial staff of the *American University International Law Review*, whose suggestions and guidance were crucial to the success of this Comment.

INTRODUCTION

On July 12, 1996, a United States-led group of thirty-three nations adopted the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar" or "The Arrangement").[1] The Arrangement purports to attain

1. *See* The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, July 11-12, 1996 [hereinafter The Wassenaar Arrangement], *reprinted in* STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST: CRYPTOGRAPHY, GOVERNMENTS, AND ELECTRONIC COMMERCE 605 (1998). The 33 countries participating in the Wassenaar Arrangement include Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech

global and regional security by promoting transparency[2] and greater responsibility in the transfer of conventional arms and dual-use goods[3] and technologies. Signatories[4] to Wassenaar agree to cooperate with each other to limit the export of conventional weapons and dual-use technologies to politically unstable nations or regions.[5] The Arrangement is non-binding and each signatory agrees to enact domestic legislation[6] to give The Arrangement its effect.[7]

Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. *See id.* at 71.

2. *See* Kenneth A. Dursht, Note, *From Containment to Cooperation: Collective Action and the Wassenaar Arrangement*, 19 CARDOZO L. REV. 1079, 1114 (1997) (defining transparency as greater and more frequent communication regarding the transfer of dual-use goods with an eye towards increasing cooperation among Wassenaar members).

3. *See* 15 C.F.R. pt. 772 (1999) (defining dual-use goods as those items that have both a commercial and military end-use).

4. *See* BAKER & HURST, *supra* note 1, at 72 (1998) (outlining the criteria for gaining membership to Wassenaar). Prospective Wassenaar members must meet the following criteria: "(1) be a producer or exporter of arms or associated dual-use goods and technology; (2) have appropriate national policies, such as not selling arms or sensitive dual-use items; (3) adhere to international proliferation norms and guidelines; and (4) implement fully effective export controls." *Id.*

5. *Compare* The Wassenaar Arrangement, *supra* note 1, sec. I, at 605-06 (stating that the purpose of The Arrangement is to limit the export of sensitive technologies to unstable countries and regions, however, The Arrangement does not specifically target any particular nation or region), *with* BAKER & HURST, *supra* note 1, at 71 (remarking that the United States had hoped the Wassenaar Arrangement would target certain rogue nations).

6. *See* The Wassenaar Arrangement, *supra* note 1, sec. III.1, at 607 ("Participating states will control all items set forth in the List . . . with the objective of preventing unauthorized transfers or re-transfers of those items."). The Arrangement also states that members will, through their domestic policies, ensure that the transfer of controlled items does not "contribute to the development or enhancement of military capabilities." *See id.* sec. I.1, at 605.

7. *See* BAKER & HURST, *supra* note 1, at 73 (noting how signatory states agreed to vigilantly uphold the items on the control list to prevent unauthorized transfers and re-transfers).

Wassenaar replaced The Coordinating Committee for Multilateral Export Controls ("COCOM"),[8] which the United States and its European allies established in 1949, as the leading international export control organization.[9] COCOM controlled the export of dual-use items to the Soviet Union and its satellites under the Industrial List.[10] The items that comprised the Industrial List were the subject of intense debate among COCOM members, as each member interpreted the meaning of the term "dual-use" in a manner consistent with their own nation's economic interests.[11] Such disagreement eventually played a role in COCOM's dismantling.[12]

Wassenaar members placed Encryption items on the original List of Dual-Use Goods and Technologies ("Dual-Use Control List").[13]

---

8. *See* Trevor Hiestand, Comment, *Swords into Plowshares: Considerations for 21st Century Export Controls in the United States*, 9 EMORY INT'L L. REV. 679, 685 (1995) (setting forth the parties to COCOM). Established in 1949, COCOM's original members included all of the members of the North Atlantic Treaty Organization ("NATO") and Finland. *See id.* At COCOM's dissolution in 1994, its members included Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Luxembourg, Japan, the Netherlands, Norway, Portugal, Spain, Turkey, the United Kingdom, and the United States. *See id.*

9. *See* Dursht, *supra* note 2, at 1098 (observing that the Soviet Union's conduct in the Berlin Crisis and the Communist takeover of China contributed significantly to the creation of COCOM); *see also* Hiestand, *supra* note 8, at 686 (noting the three purposes of COCOM as (1) promoting the creation of common export control policies among member nations, (2) processing requests by exporters for license exceptions and harmonizing member nations' oversight and enforcement policies, and (3) developing guidelines to determine the type of exports that should be considered threats to COCOM's collective security).

10. *See* Dursht, *supra* note 2, at 1099-1100 (outlining how the Industrial List controlled the export of dual-use goods and technologies amidst controversy). Because COCOM operated in such a discreet manner, it did not publish any of its control lists. *See id.* at 1100.

11. *See* Hiestand, *supra* note 8, at 687 (commenting that each COCOM member had specific economic needs and, therefore, tailored the dual-use definition to satisfy their commercial interests).

12. *See* Dursht, *supra* note 2, at 1102-03 (suggesting that COCOM's usefulness expired with the downfall of communism, as COCOM members who felt constrained by its export restrictions began establishing trade ties with Eastern Europe).

13. *See* The Wassenaar Arrangement, *supra* note 1, Category 5-pt. 2, at 614-17

Initially, the Dual-Use Control List did not place a ceiling on the strength of exported encryption products.[14] It also did not control encryption products that were generally available or in the public domain.[15] Hence, while United States encryption exporters were frustrated by domestic export policies that remained more restrictive than Wassenaar, foreign manufacturers were operating in less restrictive environments.[16]

In December 1998, Wassenaar members revised the Dual-Use Control List, implementing a maximum bit length[17] of 64-bits on exports of mass-market encryption software.[18] The Administration

---

(defining the items controlled by the Dual-Use Control List).

14. *But see* BAKER & HURST, *supra* note 1, at 76 (opining that although Wassenaar has relatively loose controls on encryption exports, it also permits members to heavily restrict encryption exports).

15. *See id.* at 74 (remarking that the failure of the United States to convince its Wassenaar allies to include generally available encrypted software has not prevented the Clinton Administration (the "Administration") from regulating the export of such software by United States companies); *infra* note 18 for a definition of generally available encryption software.

16. *See* discussion *infra* Parts III.A and III.D.

17. *See* discussion *infra* note 34 and accompanying text.

18. *See* The Wassenaar Arrangement, *supra* note 1, Category 5-pt. 2, at 613-17 (decontrolling the export of encrypted software that is generally available). The Cryptography Note to the revised List states:

> 5. A. 2 and 5. D. 2 do not control items that meet all of the following:
> a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
> 1. Over-the-counter transactions;
> 2. Mail order transactions;
> 3. Electronic transactions; or
> 4. Telephone transactions.
> b. The cryptographic functionality cannot be easily changed by the user;
> c. Designed for installation by the user without further substantial support by the supplier;
> d. Does not contain a "symmetric algorithm" employing a key length exceeding 64- bits; and
> e. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. to d. above.

See id.

claimed that the revision closed a significant loophole that previously permitted foreign companies to export mass-market software of any bit length,[19] and thereby gain a competitive edge over their United States counterparts.[20] Until Wassenaar evolves into a binding export control regime, however, current domestic policy will continue to adversely affect the ability of American exporters to remain competitive in the global encryption market. A recent proposal by the Administration to liberalize its export control regulations would, if implemented in its original form, enable domestic encryption exporters to compete with foreign encryption manufacturers.[21]

The Administration claims that Wassenaar is the preferred framework for regulating the export of encryption products.[22] Specifically, Administration officials[23] view Wassenaar as an agreement that will assist American technology companies to become more competitive in the global encryption market while protecting United States na-

---

19. *See* John Markoff, *International Group Reaches Agreement on Encryption*, N.Y. TIMES, Dec. 4, 1998, at A1 (stating that the Administration believes the revisions to the Wassenaar control lists will level the playing field between the United States and foreign encryption exporters); *see also United States Welcomes Wassenaar Decision to 'Modernize' Encryption Export Rules* [July-Dec. 1998], 15 Int'l Trade Rep. (BNA) No. 48, at 2046-47 (Dec. 9, 1998) (reiterating the Commerce Department's official statement that the revisions grant Wassenaar members the legal authority to require exporters to obtain export licenses for mass-market encryption products exceeding key lengths of 64-bits).

20. *See* Lance J. Hoffman et al., Cyberspace Policy Institute, *Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations*, June 10, 1999, at 6 (noting a 149-product increase in foreign-manufactured encryption products since December 1997); *see id.* at 36-52 (providing an exhaustive list of foreign encryption products).

21. *See infra* Part II.D (discussing the latest Administration proposal to liberalize United States export laws on encryption and provide law enforcement with additional tools to combat the use of encryption for illicit means).

22. *But see infra* Part IV.A (opining that the non-binding nature of Wassenaar frustrates any chance of it becoming an effective international export control regime).

23. *See* BAKER & HURST, *supra* note 1, at 23-24 (listing the Department of Commerce ("DOC"), including the Bureau of Export Administration ("BXA"), the Department of Justice ("DOJ"), and the Department of Defense, including the National Security Agency ("NSA"), as the Executive Branch agencies that oversee the export of encryption products for non-military end uses).

tional security interests.[24] The Administration posits that current United States policy, which in many respects mirrors Wassenaar, strikes a balance between these conflicting interests.[25] Although some Wassenaar members have reportedly shown an interest in developing such a "harmonized international approach to encryption controls,"[26] they have not yet demonstrated a desire to incorporate Wassenaar in its full form.[27]

This Comment asserts that the Administration's efforts to create an international export control regime through Wassenaar have not adequately protected United States economic interests.[28] Part I of this Comment defines encryption and examines the forces that are shaping the global encryption debate. Part II discusses and critiques United States policy towards encryption exports since Wassenaar and summarizes pending legislation, introduced separately by members of Congress and the Administration, that would liberalize United States encryption export policy. Part III asserts that Wassenaar cannot work without an enforcement mechanism, as the recent liberalization of the domestic encryption laws of various European Wassenaar members illustrate. Part IV recommends that the United States and its Wassenaar partners build on Wassenaar's current framework and develop a binding export control regime that is more inclusive and in tune with the commercial realities of the global encryption market.

Accordingly, given the current climate of liberalization and Wassenaar's inherent weaknesses, this Comment concludes that The Ar-

---

24. *See* discussion *infra* Part I.B.

25. *See The Security and Freedom Through Encryption Act: Hearings on H.R. 850 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. (Mar. 4, 1999) <http://www.house.gov/judiciary/106-22.htm> (statement of William A. Reinsch, Under Secretary for Export Administration, United States Department of Commerce) [hereinafter Reinsch Statement] (recognizing that the creation of a reliable multilateral export control regime is an evolutionary process that seeks to balance these competing interests).

26. *Id.*

27. *See* discussion *infra* Part III.D (examining the recent resistance by European Wassenaar members to sacrifice their own security interests in favor of commercial interests).

28. *See* discussion *infra* Part I.B.

rangement is an ineffective means for controlling the export of encryption products. The United States government must therefore find alternative means to achieve its dual objectives of sustaining the strength of its technology industry and satisfying the important needs of law enforcement.

I. ENCRYPTION PRIMER

A. UNDERSTANDING ENCRYPTION

Encryption can best be described as a method of storing information in an unintelligible form that can only be accessed by the intended recipient.[29] This method is utilized primarily to ensure confidentiality, promote integrity, and authenticate data.[30] The original message is referred to as plain text[31] and, once encrypted, the information becomes known as cipher text.[32] In order to encrypt a message, the sender must apply a mathematical function, known as an algorithm,[33] to that message. Within the algorithm exists a key whose

---

29. *See* Christian R. White, Comment, *Decrypting the Politics: Why the Clinton Administration's National Cryptography Policy Will Continue to be Dictated by National Economic Interest*, 7 COMMLAW CONSPECTUS 193, 194 (1999); J. Terrence Stender, Note, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 CASE W. RES. J. INT'L L. 287, 293-94 (1998) (referring to information in its unintelligible form as gibberish).

30. *See* Mai-Trâm B. Dinh, Note, *The U.S. Encryption Export Policy: Taking the Byte Out of the Debate*, 7 MINN. J. GLOBAL TRADE 375, 380 (1998) (discussing the purposes for using encryption to scramble communications). Encryption ensures the confidentiality of data by preventing third parties other than intended recipients from decrypting the message. *See id.* Additionally, encryption authenticates data by allowing a recipient to confirm that a particular sender sent the message, and ensures that the message was not altered by a third party. *See id.* Finally, encryption ensures data integrity by permitting a recipient to confirm that the message was not altered in transit. *See id.*

31. *See* Stender, *supra* note 29, at 294 (defining plain text as the original, unencrypted information).

32. *See id.* (characterizing cipher text as encrypted plain text).

33. *See* White, *supra* note 29, at 194 (noting that an algorithm is an ordered set of mathematical instructions used in the process of encrypting and decrypting); *see also* BAKER & HURST, *supra* note 1, at 4 (comparing the algorithm to a lock on a safe).

bit length,[34] in addition to the complexity of the algorithm, determines the strength of the encryption.[35] Absent a brutal assault by hackers, or third party access by key escrow[36] agents, the intended recipient of the key is the only person capable of decrypting[37] the scrambled message. Accordingly, the person sending the encrypted message places a great degree of trust in the intended recipient that his communication will remain confidential.[38]

---

34. *See* Dinh, *supra* note 30, at 379-80 (demonstrating the effect of adding additional bits to a key). For instance, a 40-bit key provides over one trillion potential combinations while seventy-two quadrillion combinations exist for a 56-bit key. *See id.*

35. *See* BAKER & HURST, *supra* note 1, at 4 (noting that the greater the key bits, the more difficult it becomes for third parties to unscramble the encrypted message). *But see* Stender, *supra* note 29, at 297 (demonstrating that the length of the key does not guarantee security, as weaknesses in key management protocols or implementation can allow keys to be cracked rather quickly). For example, students at the University of California at Berkeley found that the encryption key used by the Netscape Internet browser was easy to hack because it was not sufficiently random. *See id.* at 297 n.47; *see also* Bernadette Barnard, Note, *Leveraging Worldwide Encryption Standards Via U.S. Export Controls: The U.S. Government's Authority to "Safeguard" the Global Information Infrastructure*, 1997 COLUM. BUS. L. REV. 429, 435 (1997) (stating that if the algorithm is not complex enough, a weakness can be exploited to reduce the number of possible combinations required to crack the encrypted message).

36. *See* NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 168 (Kenneth W. Dam & Herbert S. Lin eds., 1996) (defining escrowed encryption as the placing of the key with a trusted third party for the purpose of assuring law enforcement access to encrypted materials when authorized under law, and as a mechanism for protecting against lost, corrupted, or unavailable keys); *see also* Stender, *supra* note 29, at 298-99 (stating that the term "escrow" was first introduced in 1993 by the Administration to aid law enforcement in gaining access to encrypted voice communication from wiretaps); M. Christopher Bolen & Donna R. Chmura, *Usinessbay Eedsnay Ecretsay Odescay*, NAT'L L.J., Nov. 11, 1996, at A17 (stating that the terms key escrow and key recovery are synonymous).

37. *See* White, *supra* note 29, at 194 (defining decryption as the way in which cipher text becomes readable to the intended recipient).

38. *See* BAKER & HURST, *supra* note 1, at 5 (illustrating the vast uncertainties implied in Internet usage).

B. BALANCING COMPETITIVENESS AND NATIONAL SECURITY NEEDS

United States computer software and hardware manufacturers,[39] in conjunction with various trade associations,[40] are among the groups that are lobbying before Congress and the Administration for greater export liberalization for encryption products.[41] Presently, United States Export Administration Regulations[42] ("EARs") only permit the unrestricted export of encryption products with up to 56-bit encryption,[43] with some exceptions.[44] Foreign software manufacturers have capitalized on this burdensome policy by developing software with 128-bit encryption or higher.[45] These foreign businesses have flourished as the demand for maximum security in on-line transactions continues to increase.[46] Meanwhile, United States firms are losing

---

39. *See generally* William Larson, *News Conference at the Business Software Alliance* (June 16, 1999), *available in* LEXIS, Legis Library, Poltrn File (statements of William Larson, Chairman and CEO, Network Associates, Inc., and Eric Schmidt, Chairman and CEO, Novell, Inc.).

40. *See generally Emerging Technology Issues and Reauthorization of the Export Administration Act: Hearings Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 106th Cong. (June 17, 1999) <http://banking.senate.gov/99_06hrg/061779/hirschhn.htm> (statement of Eric L. Hirschhorn, Executive Secretary, Industry Coalition on Technology Transfer) (providing examples of the industry associations that are lobbying Congress and the Administration on behalf of the United States technology industry).

41. *See* 15 C.F.R. sec. 772 (defining encryption products as all encryption commodities, software, and technology that contain encryption features and are subject to the EARs). Such items exclude encryption items designed, configured, adapted, or modified solely for military use that are controlled by the Department of State on the United States Munitions List. *See id.*

42. 15 C.F.R. secs. 730-772 (1999).

43. 15 C.F.R. sec. 742.15 (1999) (setting forth the key provisions of the interim rule).

44. *See infra* notes 89-92 and accompanying text (discussing the types of exports that are exempt from regulation by the BXA).

45. *See* Hoffman, *supra* note 20, at 6 (identifying a total of 805 encryption products manufactured in 35 countries as of May 1999).

46. *See The Need for Fundamental Reform of America's Encryption Policy: Hearings on S. 798 Before the Senate Comm. on Commerce, Science, and Transportation*, 106th Cong. (1999), *available in* 1999 WL 395654 (statement of David Aucsmith, Chief Security Architect, Intel Corporation) [hereinafter Aucsmith

billions of dollars in the global software market.[47] At the opposite end of the spectrum, the Administration and law enforcement agencies oppose further deregulation for fear that it would hamper domestic and international crime interdiction efforts.[48] Additionally, the Administration asserts that further liberalization is inconsistent with Wassenaar's principles.[49]

1. The Technology Industry Perspective

United States exporters base their opposition to export controls on encryption products on several grounds. First, United States exporters argue that such controls harm United States economic interests by allowing foreign manufacturers to gain significant market share, thereby placing much of the research and development in the hands

---

Statement] (remarking that the increased reliance of individuals upon secure infrastructures and the increased desire of governments to protect those infrastructures will lead to a greater need for strong encryption). Furthermore, Aucsmith states that "it is only a matter of time before strong encryption becomes a commodity feature of global networks and information systems." *See id.*

47. *See* White, *supra* note 29, at 193 (estimating that current export policies will result in losses of $60 billion to United States software manufacturers); Kimberly A. Strassel, *On Hold with James Bond*, WALL ST. J. EUR., June 30, 1998, *available in* 1998 WL-WSJE 12725941 (citing a survey, which estimates that the United States technology industry will lose $60 billion in revenue and 200,000 jobs by 2002 due to encryption controls).

48. *See Encryption and Export Security: Hearings on H.R. 850 Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (1999), *available in* 1999 WL 503726 (statement of Janet Reno, Attorney General, United States Department of Justice) [hereinafter Reno Statement] (remarking that the widespread use of encryption without third party access capabilities will prevent law enforcement from obtaining information needed to protect the public safety); *Encryption and Export Security: Hearings on H.R. 850 Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (1999), *available in* 1999 WL 503728 (statement of Louis J. Freeh, Director, Federal Bureau of Investigation ("FBI")) [hereinafter Freeh Statement] (remarking that the law enforcement agencies are in unanimous agreement that the use of strong and non-recoverable encryption will seriously hamper law enforcement's ability to fight crime). Freeh also remarked that 28 of the FBI's 56 nationwide field offices have encountered the use of encryption in cases of violent crime and white-collar crime. *See id.*

49. *See* Reinsch Statement, *supra* note 25 (asserting the Administration's commitment towards promoting an effective international export regime through the Wassenaar Agreement).

of foreign nations.[50] For instance, it is well documented that European software manufacturers, most notably Brokat Information Systems AG[51] and Baltimore Technologies,[52] have won lucrative contracts over their United States counterparts to provide European corporations with encryption software and services.[53] In addition,

---

50. *See Telecommunications, Trade and Consumer Protection: Hearings on H.R. 850 Before the House Subcomm. of the Comm. on Commerce*, 106th Cong. (1999), *available in* 1999 WL 332217 (statement of Richard Hornstein, Vice President, Legal Affairs, Taxation and Corporate Development, Network Associates, Inc.) [hereinafter Hornstein Statement] (remarking that hundreds of encryption products are currently being developed offshore by foreign manufacturers); *see also Encryption: Security in a High Tech Area: Hearings on H.R. 850 Before the Subcomm. on International Economic Policy and Trade of the House Comm. on International Relations*, 106th Cong. (1999), *available in* 1999 WL 314028 (statement of Edward J. Black, President & CEO, Computer and Communications Industry Association) [hereinafter Black Statement] (asserting that the Administration's policy is illogical because there is no proven market for encryption products with key recovery features).

51. *See* Strassel, *supra* note 47, at 1 (attributing Brokat's immediate success, since its founding in 1994, to restrictive United States export policies). Brokat now serves approximately 1,400 customers, and has expanded its business to non-encryption products. *See id.*; *see also* Hoffman, *supra* note 20, at 3 (discussing the 1998 report of the President's Export Council Subcommittee on Encryption ("PECSENC"), which cited Brokat's success as an example of the adverse impact that United States export policies have on the ability of American firms to remain competitive in the global encryption market). Specifically, the 1998 report stated:

> Brokat, a German company that scarcely existed four years ago, now has 250 employees and offices in several countries including the United States . . . It is now a major player in [the encryption market], with 50% of the European Internet banking market and enough United States customers to justify a 20-person United States branch office.

See id. (alteration in original).

52. *See* Strassel, *supra* note 47, at 1 (providing as an example a European Union-funded project called MIPEX, which required encryption software to link several patent offices throughout Europe, and hired Baltimore Technologies, a Dublin based company, to provide such products and services). The European Commission has purchased approximately $100,000 worth of encryption software from Baltimore Technologies. *See id.*

53. *See id.* (noting that United States technology giants such as Microsoft and RSA Data Security ("RSA") have begrudgingly turned down lucrative contracts to provide strong encryption to European companies because of restrictive United States export control policies). For example, Consensus Development Corporation,

United States technology industry representatives maintain that current United States policy compromises United States national security interests by forcing law enforcement to decode encryption designed and manufactured exclusively by foreign corporations.[53] Finally, exporters maintain that export controls place financial systems and valuable intellectual property at risk.[54]

2. The National Security Perspective

The Administration and the law enforcement community, on the other hand, oppose further liberalization of the EARs without a key recovery or escrow option.[56] Such fears are based on the potential for harm to the nation's security interests.[57] Essentially, law enforcement

---

which licenses encryption software to technology giants such as IBM, claims that it loses approximately 40% of its sales leads because they turn out to be foreign companies. As a result, the Chief Executive of RSA states that United States firms feel that the encryption market that they and their United States partners created has been "handed on a silver platter to the rest of the world." *See id.*; *see also* Aucsmith Statement, *supra* note 46, at 173 (quoting a recent statement by the European Commission, which acknowledged that current United States export control laws provide good opportunities for European companies to enter the global encryption market).

54. *See The United States Needs a Clear and Realistic Encryption Policy: Hearings on H.R. 850 Before the Subcomm. on International Economic Policy and Trade of the House Comm. on International Relations*, 106th Cong. (1999), *available in* 1999 WL 314030 (statement of Jeffrey H. Smith, Counsel, Americans for Computer Privacy) [hereinafter Smith Statement] (remarking that if the United States loses its leadership position in the global technology market, United States national security agencies will have to obtain technical assistance from foreign sources, which Smith believes is unacceptable).

55. *See* E. Franklin Haignere, Comment, *An Overview of the Issues Surrounding the Encryption Exportation Debate, Their Ramifications, and Potential Resolution*, 22 MD. J. INT'L L. & TRADE 319, 327 (1998-99) (outlining the key arguments in the encryption debate).

56. *See supra* note 36 and accompanying text (defining key recovery and key escrow).

57. *See* Stender, *supra* note 29, at 322 (recognizing that although strong encryption is available from non-United States sources, the Clinton Administration does not want to contribute to the proliferation of such products); *see also* H.R. REP. NO. 106-117, pt. 1, at 19 (1999) (outlining the government's options in regard to encryption regulation). The FBI, Central Intelligence Agency ("CIA"), and Drug Enforcement Administration ("DEA") view the debate as between (1) those who

advocates argue that widespread use of encryption would hamper intelligence gathering and undermine the ability of law enforcement to prevent crime.[58] A recently published Federal Bureau of Investigation ("FBI") report[59] states that "[e]ncryption can also be used to conceal criminal activity and thwart law enforcement efforts to collect critical evidence needed to prevent, solve and prosecute serious and often violent criminal activities, including illegal drug trafficking, organized crime, child pornography, and terrorism."[60] For instance, law enforcement officials cite examples where strong encryption frustrated court-authorized crime interdiction efforts.[61] Recent terrorist incidents also heighten fears that strong encryption has already become a vital tool used by terrorists[62] and drug cartels[63] to evade detection by law enforcement officials.

---

are in favor of strong encryption that protects commerce but gives criminals a new weapon and (2) those who also favor strong encryption but with an escrow option that protects the public interest. *See id.*

58. *See* Stender, *supra* note 29, at 326 (suggesting that intelligence-gathering is an essential component of combating terrorism abroad and within the United States).

59. *See generally* FBI, ENCRYPTION: IMPACT ON LAW ENFORCEMENT (1999), at 1-17 (outlining the devastating effect that the widespread use of encryption products would have on crime prevention).

60. *Id.* at 5.

61. *See* H.R. REP. NO. 106-117, pt. 1, at 20 (1999) (citing an increase in the number of instances in which the FBI and the DEA's court-authorized electronic surveillance efforts were thwarted by criminals' use of strong encryption).

62. *See* Stender, *supra* note 29, at 329 (pointing to World Trade Center bomber Ramzi Yousef's use of encryption to protect computer files relating to his terrorist activities); *see also* Jim Walsh, *Reno Seeks 'Key' to Foil Online Crime; Device Could Curb Computer Thievery*, ARIZ. REPUBLIC, Oct. 29, 1996, at B1 (quoting an FBI encryption expert who found encrypted files containing plans for 11 terrorist attacks saved on Yousef's laptop computer).

63. *See Encryption and Export Security: Hearings on H.R. 850 Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (1999), *available in* 1999 WL 503735 (statement of Thomas A. Constantine, Former Administrator, DEA) (stating that "[t]o the extent that the communications of these groups are placed beyond our reach by encrypted communications . . . we will be severely hindered to make cases against the leadership and United States-based infrastructure of [drug cartels].")

II. UNITED STATES ENCRYPTION POLICY

A. PRESIDENT CLINTON'S 1996 EXECUTIVE ORDER

On November 15, 1996, President Clinton issued an Executive Order[64] transferring jurisdiction over encryption products named as defense articles on the United States Munitions List[65] to the Department of Commerce's Commerce Control List ("CCL").[66] President Clinton included certain mass-market[67] encryption products among the items he authorized for transfer to the CCL.[68] The Executive Order excluded encryption products from the sections of the Export Administration Act ("EAA")[69] governing controls on goods or technology that are generally available outside the United States.[70] The

---

64. *See* Exec. Order No. 13,026, 61 Fed. Reg. 58,767-68 (1996), *reprinted in* 50 App. U.S.C. sec. 2403 (1999) [hereinafter Exec. Order No. 13,026] (amending the Export Administration Regulations ("EARs")).

65. *See* 22 C.F.R. sec. 121.1 (1995) (categorizing encryption products under Category XIII to the Munitions List).

66. *See* Exec. Order No. 13,026, *supra* note 64, at 58,768 (determining that the export of encryption products could harm national security interests even where similar products are freely available from non-United States sources); *see also* 15 C.F.R. sec. 744, Supp. No. 1 (1999) (stating that encryption hardware and software are controlled by the DOC under CCL categories 5A002, 5D002, respectively).

67. *See* 15 C.F.R. sec. 742(a) (1997) (defining mass-market encryption products as those that are publicly available from retailers, whether by over-the-counter, mail, or telephone transactions, that are user-friendly and do not require substantial technical support, including encryption for confidentiality purposes).

68. *See* 61 Fed. Reg. 68,581 (1996) (interim rule adopted as of Dec. 30, 1996) (amending sec. 742.15(b)(1) of the Export Administration Regulations to include 40-bit mass-market encryption software among the items transferred from the United States Munitions List to the CCL).

69. 22 U.S.C. sec. 2401 (1999).

70. *See* 50 U.S.C. app. sec. 2403(c) (1999). This section states:

> [T]he President shall not impose export controls for foreign policy or national security purposes on the export from the United States of goods or technology which he determines are available without restriction from sources outside the United States *in sufficient quantities and comparable to those produced in the United States* . . . unless the President determines that adequate evidence has been presented to him demonstrating that the absence of such controls would prove detrimental to the foreign policy or national security of the United

Executive Order also permitted export control regulations to include provisions promoting the development of a key recovery system.[71] Finally, pursuant to the Executive Order, President Clinton appointed a Special Envoy for Cryptography[72] to develop a global encryption policy modeled after that of the United States.

1. Promoting Mandatory Key Escrow

The Executive Order promoted the use of key escrow as a way of allowing law enforcement[73] to gain access to encrypted messages.[74] The Administration hailed its key escrow policy as a means of preserving the interests of both law enforcement and United States exporters.[75] The updated policy placed the mandate in the hands of the

---

States.

See id. (emphasis added); *see also* 50 U.S.C. app. sec. 2405(h)(2-4) (requiring the President, pursuant to negotiations with foreign governments, to report the possible consequences of proposed export controls to Congress); *Letter to Congressional Leaders on Encryption Products Export Controls*, 2 PUB. PAPERS 2123 (Nov. 15, 1996) (remarking that any EAA provisions that grant export licenses or remove controls on encryption products based on foreign availability shall not apply).

71. *See* Exec. Order No. 13,026, *supra* note 64, at 58,768 (listing some of the controls on the export of encryption products).

72. *See Gore Announces Special Envoy for Cryptography*, U.S. NEWSWIRE, Nov. 15, 1996, *available in* LEXIS, News Library, USNWR File (announcing Ambassador David Aaron as the United States' Special Envoy for Cryptography). President Clinton gave Ambassador Aaron the responsibility of promoting the "growth of international electronic commerce and robust, secure global communications in a manner that protects the public safety and national security." *See id.*

73. *See* Stender, *supra* note 29, at 297 (stating that the key could be released to authorized parties, subject to either a court order or predetermined by the messenger or government).

74. *See* Walsh, *supra* note 62, at B1 (discussing Reno's desires to provide police with an electronic key to seize encrypted evidence and gain the upper hand in preventing high-tech crime).

75. *See* NATIONAL RESEARCH COUNCIL, *supra* note 36, at 177-78 (discussing the Administration's 1996 proposal to increase the exportable encryption levels to 64-bit on products with escrow features embedded in them and providing a brief outline of the Administration's 1996 proposed key recovery policy); *see also* Stender, *supra* note 29, at 308 (discussing the Administration's conditioning of permission to export non-recovery 56-bit encryption products for two years on corporation promises to develop encryption products with escrow features).

industry to develop key escrow systems."[76] Under this new policy, the Bureau of Export Administration ("BXA") granted license exceptions[77] to corporations that agreed to develop key escrow systems within the next two years.[78] Additional concessions permitted organizations to designate one or more employees, instead of government employees, as escrow agents.[79] Although industry leaders viewed this as a positive step towards liberalization,[80] many expressed concerns that the policy provided little relief for exporters competing with foreign encryption suppliers.[81]

---

76. *See RSA Optimistic on User Benefits of Administration's Recent Key Recovery Initiative Announcement*, Business Wire, Oct. 4, 1996, *available in* LEXIS, News Library, Bwire File (surmising that placing such a mandate in the hands of industry will result in more effective solutions to key escrow); *HP Attacks Internet International Security Vulnerability Issues*, Business Wire, Nov. 18, 1996, *available in* LEXIS, News Library, Bwire File (detailing Hewlett-Packard's plan to implement a government-approved International Cryptography Framework, which would provide encryption users with varying levels of encryption depending on the type of data being encrypted and the jurisdiction in which it is being used); *see also* Bolen & Chmura, *supra* note 36, at A17 (describing IBM's response to the Executive Order with a plan to develop key recovery systems that would meet the requirements of business and ease import and export restrictions on encryption products worldwide).

77. *See* Mark Felsenthal, *Administration Steps Up Drive to Export Software With Strong Encryption Capability*, Int'l Trade Daily Rep. (BNA) (Sept. 17, 1998), *available in* LEXIS, BNA Library, BNAINTD File (defining license exception as the procedure by which encryption products are permitted to be freely exported following a one-time review).

78. *See* Black Statement, *supra* note 50 (summarizing the Administration's 1996 key escrow policy).

79. See 15 C.F.R. sec. 742, Supp. No. 5 (1997) (outlining the safeguards necessary to approve the use of internal key recovery agents). According to the EARs, such safeguards should ensure the agent's structural independence from the rest of the organization, security, and confidentiality. *See id.*

80. *See RSA Optimistic on User Benefits of Administration's Recent Key Recovery Initiative Announcement*, *supra* note 76 (noting that although the Administration's reforms are a positive first step, they fail to provide relief to United States exporters competing with foreign manufacturers who can export non-recoverable encryption products with greater security).

81. *See id.* (stating that foreign suppliers, who are not subject to United States law, can provide non-recovery encryption in their products); Conrad Burns, *Development of Internet Services Hurt by Export Encryption Technology*, N.Y. L.J., Oct.

2. Victories for the Law Enforcement Community

President Clinton's Executive Order, while providing key concessions to exporters, strengthened law enforcement's influence over the BXA licensing process.[82] First, the Executive Order granted to the Department of Justice ("DOJ") and its law enforcement bureaus greater power over the administration of export licenses.[83] Second, the revised BXA regulations required escrow agents to meet strict eligibility standards,[84] signaling the Administration's commitment to

---

15, 1996, at 7 (reporting that "[n]o matter how stringent United States encryption export controls are, they can do nothing to stop a bright mathematician in Tokyo, Paris or Bonn . . . from developing robust encryption and offering it for worldwide distribution."). Senator Burns provides as an example Nippon Telephone & Telegraph's 1996 announcement that it would soon offer for global distribution an encryption chip with significantly stronger encryption than the United States government currently permits its companies to export. *See id.* Accordingly, United States companies may soon have to confront the choice of moving their business offshore or conceding defeat to foreign encryption manufacturers. *See id.*

82. *See* BAKER & HURST, *supra* note 1, at 18 (commenting that the 1996 policy gave the DOJ a hand in export decisions concerning encryption products).

83. *See* Exec. Order No. 13,026, *supra* note 64, at 58,767-68 (granting to the DOJ the opportunity to review any export license application under review by the DOC). President Clinton further amended Exec. Order No. 12,981, promulgated on December 5, 1995, authorizing the DOJ to become a voting member of the Export Administration Review Board and of the Advisory Committee on Export Policy with respect to encryption products. *See id.*; *see also* BAKER & HURST, *supra* note 1, at 18 (stating that President Clinton granted the DOJ a greater role in encryption export determinations); *see generally Export Licensing for Dual-Use Technology, Before the Subcomm. on Int'l Trade and Fin. of the Senate Cmm. on Banking, Housing, and Urban Affairs*, 106th Cong. (Apr. 14, 1999) (statement of R. Roger Majak, Assistant Secretary for Export Administration, Department of Commerce) <http://www.bxa.doc.gov/press/99/MajakDualUseTech.html> (commenting on the advantages in involving a greater number of agencies in the export licensing process). DOC officials argue that increasing the number of agencies involved in the decision-making process (1) ensures that more facts and opinions will be considered in each case, (2) encourages more timely and efficient decision-making, and (3) permits cases that raise policy issues, factual inconsistencies, and sharp disagreement to be reviewed at the highest levels of government. *See id.*

84. *See* 15 C.F.R. sec. 742.15, Supp. No. 5 (1997) (outlining the standards by which eligible key recovery agents are measured). Evidence of a prospective agent's suitability is determined by information demonstrating that the candidate: (1) has no criminal record or any charges pending against him or her, (2) has not

creating an export control policy that serves the needs of law enforcement.[85] As for the latter point, the Administration continues to cooperate with high-technology firms to develop recoverable encryption software in which the private third party, and not the government, holds the decryption keys.[86]

B. SECTORAL LIBERALIZATION

On September 16, 1998, Vice President Gore announced a revised Administration policy on encryption.[87] The Administration changed its policy with respect to three areas. First, it made permanent the permission to export 56-bit encryption products after a one-time technical review by the BXA.[88] Second, it permitted the export of encryption products with limitless encryption capabilities to a number of industrial sectors, including banking and financial institutions,[89] on-line merchants,[90] and health and medical organizations[91] in all na-

---

breached any fiduciary obligations, and (3) is creditworthy. *See id.* Absent the above preconditions, an eligible candidate must have a current United States Government security clearance of secret or higher. *See id.*

85. *See* Albert Gore, *News Briefing on Encryption* (Sept. 16, 1998), *available in* 1998 WL 634722 (publicizing the new export control policy as a balance between protecting the growth of electronic commerce with the technological needs of law enforcement to fight modern crime).

86. *See HP Attacks Internet International Security Vulnerability Issues*, *supra* note 76 (detailing Hewlett-Packard's government-sponsored International Cryptography Framework).

87. *See* Gore, *supra* note 85 (remarking that the new policy will allow American corporations to use encryption programs of unlimited strength when communicating with most countries).

88. *See* Felsenthal, *supra* note 77 (adding that the Administration removed the key recovery requirement in exchange for promises by individual corporations to develop key recovery systems). In addition, the government eliminated the need for biannual status reports on the development of key recovery systems. *See id.*; *see also* Stewart A. Baker & Elizabeth A. Banker, *The New Encryption Export Policy: The U.S. Govt. Rethinks Key Recovery*, 782 PLI/COMM. 589, 601 (1998) (stating that the new policy creates less incentive for the technology industry to develop key recovery systems).

89. *See* 15 C.F.R. sec. 742.15(b)(3) (1999) (permitting the unrestricted export of general-purpose encryption commodities and software of any bit length).

90. *See* 15 C.F.R. sec. 742.15(b)(6) (1999) (limiting the use of encryption

tions except those subject to United States embargoes.[92] Finally, the new policy expanded export opportunities by granting license exceptions for exports to such entities after a one-time technical review.[93] Proponents of liberalization had mixed reactions to the new policy.[94] The government, however, promoted this policy shift as a victory for both law enforcement and business groups.[95]

C. CURRENT LEGISLATIVE CHALLENGES TO UNITED STATES ENCRYPTION POLICY

1. SAFE Act

Recently, the House Judiciary Committee[96] and House Commerce

---

commodities and software to on-line transactions). Specifically, the EARs limit on-line merchants' use of encryption to the purchase or sale of goods and software, including any services rendered in connection with the ordering and payment for such purchases. *See id.*

91. *See* 15 C.F.R. sec. 742.15(b)(5) (1999) (excluding non-United States pharmaceutical and biochemical manufacturers and non-United States military health and medical entities from the list of permitted end-users).

92. *See* Baker & Banker, *supra* note 88, at 600 (stating that the new policy permits the export of encryption products regardless of strength to financial institutions, on-line merchants, and health and medical organizations (excluding biomedical and pharmaceutical manufacturers) in all countries except the embargoed nations—Cuba, Iran, Libya, North Korea, Sudan, and Syria). The policy also deregulates the export of encryption products to subsidiaries of United States companies to all nations except the embargoed nations. *See id.* at 599.

93. *See id.* at 599 (noting that encryption hardware or software exports will occur pursuant to a license exception).

94. *See* John Borland, *U.S. Crypto-Export Plan Gets Mixed Reviews*, TechWeb News, Sept. 16, 1998, *available in* LEXIS, News Library, Techwb File (suggesting that industry groups were more pleased by the Administration's policy than privacy groups). Privacy groups were disappointed that the Administration failed to abandon the key recovery idea. *See id.*

95. *See* Gore, *supra* note 85 (remarking that United States encryption manufacturers will be able to export encryption products with higher levels of encryption while still allowing law enforcement to fight terrorism).

96. *See* H.R. REP. NO. 106-117, pt. 1, at 1 (1999) (recommending that the Security and Freedom Through Encryption (SAFE) Act (the "SAFE Act") pass without amendment).

Committee[97] endorsed legislation that would liberalize United States export control laws concerning encryption. The Security and Freedom Through Encryption (SAFE) Act (the "SAFE Act"),[98] sponsored by Virginia Congressman Bob Goodlatte,[99] proposes to amend the EAA by removing altogether export controls on encryption products that are generally available[100] in the public domain[101] or embedded in consumer products not designed for military end-use.[102] The BXA would grant license exceptions to such products pursuant to a one-

---

97. *See* Robert MacMillan, *Commerce Committees SAFEly PROTECT Crypto Bills*, NEWSBYTES, June 23, 1999, *available in* LEXIS, News Library, Nwsbyt File (stating that the SAFE Act finally gained passage by a voice vote following an intense debate over proposed amendments). The Commerce Committee passed the SAFE Act in substantially the same form while adding six amendments. *See id.*; *see also House Commerce Committee Clears Encryption Bill*, National Journal's CongressDaily, June 24, 1999, *available in* LEXIS, News Library, Cngdly File (discussing two proposed amendments to the SAFE Act, including an amendment that would impose criminal penalties against escrow agents who refuse to unscramble encrypted information when required by a court order).

98. *See* H.R. 850, 106th Cong. (1999) (stating that the SAFE Act has thus far received 205 cosponsors during the 106th Congress); *see also Digital Jam: SAFE Bill Discussed* (CNNfn television broadcast, Feb. 26, 1999).

99. *See* Stender, *supra* note 29, at 310 (noting that Republican Congressman Goodlatte originally introduced the bill in 1996 in substantially the same form). Goodlatte argues that the proposed legislation serves to "prevent economic crime, promote electronic commerce, and protect the personal privacy of all law-abiding Americans." *See* H.R. REP. NO. 106-117, pt. 1, at 30 (1999).

100. *See* Security and Freedom Through Encryption (SAFE) Act, H.R. 850, 106th Cong. sec. 3(a)(4)(B) (1999) (defining the term generally available). The SAFE Act defines generally available encryption products as, among other things, computer hardware or software that are (1) available on the Internet, (2) offered for sale, licensing, or transfer to any person, (3) included with the purchase of computer hardware or software that is publicly available, or (4) assembled from computer hardware or software components that are publicly available. *See id.* sec. 3(a)(4)(B)(i)(I)-(IV).

101. *See id.* sec. 3(a)(2)(A)(i)-(ii) (stating that encryption products in the public domain include those not protected by United States copyright laws or those that are generally accessible in any form).

102. *See id.* sec. 3(a)(2)(A)(iii)(I)-(II) (including, among other items, those with encryption capabilities that are neither accessible to the end user nor designed for non-civilian uses).

time fifteen-day technical review.[103] Furthermore, the proposed legislation would prohibit federal and state governments from conditioning export approval on the implementation of mandatory key escrow systems.[104] Other key provisions of the proposed legislation would impose criminal penalties on felons who use encryption to further their illegal activities.[105] The SAFE Act, however, would retain the President's authority to prohibit the export of encryption products that are known to support acts of international terrorism and to impose embargoes on exports to a particular country.[106]

Key congressional leaders, the Administration, and law enforcement officials, whose support is vital to the SAFE Act's passage, argue that the bill compromises law enforcement and national security interests.[107] In Congress, the House Armed Services Committee, finding that the SAFE Act would threaten the national security of the United States,[108] recently gutted the bill by inserting various amend-

---

103. *See id.* sec. 3(a)(3).

104. *See id.* sec. 2(a) (proposing amendments to 18 U.S.C. sec. 2804). However, the SAFE Act preserves the right of law enforcement officers or members of the intelligence community, acting under current law, to access encrypted communications or data. *See id.*

105. *See id.* (penalizing any person who knowingly and willfully encrypts data or communications relating to the felony with intent to conceal the encrypted information so as to avoid detection by law enforcement officials. First-time offenders would face prison sentences of up to five years, with an additional five years added on for second and subsequent offenses). *See id.* However, this section makes clear that a person's use of encryption shall never be the sole basis for establishing probable cause. *See id.*

106. *See* Security and Freedom Through Encryption (SAFE) Act, H.R. 850, 106th Cong. sec. 3(c)(1) (preserving the President's power to act under the International Emergency Economic Powers Act, the Trading with the Enemy Act, or the Export Administration Act of 1979).

107. *See* Gary G. Yerkey, *Rep. Gilman Joins Administration to Oppose Bill to Loosen Encryption Controls*, 16 Int'l Trade Rep. (BNA) No. 20, at 837-38 (May 19, 1999) (reiterating the Administration's position and stating that Congressman Benjamin Gilman, Chairman of the House International Relations Committee, opposes the SAFE Act for fear it would make encryption more available to United States adversaries).

108. *See* H.R. REP. NO. 106-117, pt. 4, at 8 (1999) (supporting its conclusion that the SAFE Act, in its original form, would harm United States national security interests with statements and testimony by DOC, NSA, and other law enforcement

ments that would undermine the SAFE Act's original intent.[109] The House Judiciary Committee recently determined, however, that the SAFE Act would actually prevent crime.[110] Law enforcement agencies assert that the current version of the bill fails to address their needs because it abandons key recovery altogether.[111] Such agencies and the Administration seek cooperation from the technology industry in developing encryption products with third party access.[112] Furthermore, Administration officials allege that the bill contravenes its international export obligations under Wassenaar.[113] Conversely, representatives of the technology industry assert that SAFE is consistent

---

officials).

109. *See* Bob Woods, *Various SAFE Acts Move to House Rules Cmte.*, Newsbytes, July 22, 1999, *available in* LEXIS, News Library, Nwsbyt File (noting that the Armed Services Committee's suggested amendments granting the President the power to control the export of all dual-use encryption products, deny exports of encryption products that run counter to national security interests, and prevent judicial review of any presidential decisions in this area). One interesting observation is that the amendments did not include a key recovery provision. *See id.*; *see also* H.R. REP. NO. 106-117, pt. 4, at 9-10 (1999) (proposing that the SAFE Act grant the President the power to control the export of encryption products and permit the President to establish the maximum encryption strength for encryption exports).

110. *See* H.R. REP. NO. 106-117, pt. 1, at 2 (1999) (remarking that the use of strong encryption will protect Americans from crime, economic espionage, and information warfare). The Judiciary Committee reported that the SAFE Act struck an appropriate balance by allowing the marketplace to develop key recovery systems while tightly regulating United States export control laws. *See id.*

111. *See generally* H.R. REP. NO. 106-117, pt. 1, at 14-23 (1999) (providing examples of the opposition to the SAFE Act by various state, federal, and international law enforcement entities).

112. *See Encryption and Export Security: Hearings on H.R. 850 Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (1999), *available in* 1999 WL 503730 (statement of John J. Hamre, Deputy Secretary of Defense) (remarking that the SAFE Act would inhibit the development of key recovery by corporations that require total access to their information, and would impact the Federal government's plans to use recoverable encryption products); *see also* Freeh Statement, *supra* note 48 (remarking that a viable encryption policy should not be solely determined by the technology industry because it is not purely a business issue).

113. *See* Reinsch Statement, *supra* note 25 (stressing the Administration's dedication to developing a strong international export regime through the Wassenaar Arrangement).

with Wassenaar because it would only decontrol the export of mass-market encryption products.[114]

2. PROTECT Act of 1999

In April 1999, Arizona Senator John McCain introduced a more restrictive bill that would permit the export of encryption products utilizing key lengths of up to 64-bits.[115] Encryption items that exceed the 64-bit threshold would be exportable under a license exception where such products are generally or publicly available, or when a similar product using an identical or greater bit length becomes available from a foreign supplier.[116] At the same time, the bill acknowledges the importance of replacing the current Data Encryption Standard ("DES")[117] with the more comprehensive Advanced Encryption Standard ("AES"), which was developed in the private sector.[118] The deadline for the introduction of the AES is January 1,

---

114. *See* Hornstein Statement, *supra* note 50 (arguing that SAFE's proposed limits on encryption exports do not conflict with Wassenaar because The Arrangement only permits, and does not require the control of, 56-bit level or more mass-market encryption products).

115. *See* Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999, S. 798, 106th Cong. sec. 2 (stating that the bill's purposes include: (1) the promotion of and increasing consumers' confidence in electronic commerce; (2) meeting the needs of individuals and enterprises using on-line networks; and (3) preventing crime and improving national security); *see also* John McCain, *Encryption Bill*, FDCH Congressional Press Releases, June 24, 1999, *available in* LEXIS, Legis Library, Hillpr File (summarizing the PROTECT Act's key provisions).

116. *See* Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999, S. 798, 106th Cong. Tit. 5, sec. 505(b) (setting forth the requirements to establish an Encryption Export Advisory Board ("EEAB")). The twelve member EEAB will consist of Presidential appointees from the NSA, the CIA, the Office of the President, and the private sector. *See id.* at Tit. V, sec. 505(b)(1)(B)(i)-(iv). The EEAB's purpose will be to review applications for license exceptions based on general, public, or foreign availability. *See id.* at Tit. V, sec. 505(b)(2).

117. *See* NATIONAL RESEARCH COUNCIL, *supra* note 36, at 71 n.31 (defining the DES, which is the current standard for encrypting communications utilizing 56-bit encryption).

118. *See* Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999, S. 798, 106th Cong. sec. 3(14) (anticipating that

2002, upon which the exportable encryption level will rise to 128-bits.[119] Moreover, the PROTECT Act authorizes the export of encryption products to the strategic partners of United States exporters,[120] and members of the North Atlantic Treaty Organization ("NATO"), the Organization for Economic Cooperation and Development ("OECD"), and the Association of Southeast Asian Nations ("ASEAN"). Such exports, however, are subject to a license exception.[121]

D. RECENTLY PROPOSED ADMINISTRATION REFORMS AND THE CYBERSPACE ELECTRONIC SECURITY ACT

On September 16, 1999, exactly one year after the liberalization of United States encryption export control laws, the Administration announced a new series of reforms, scheduled to be implemented by December 15, 1999.[122] The new policy purports to remove many of

---

the AES will eventually become the international encryption standard adopted by all encryption users).

119. *See id.* sec. 3(18), Tit. V, sec. 506 (permitting United States encryption products that incorporate AES to be exported free and clear of export controls).

120. *See id.* Tit. 505, sec. 504(a)(2)(A)-(G) (describing strategic partners as: (1) publicly-held firms; (2) firms subject to a government regulatory scheme; (3) United States subsidiaries or affiliates of United States corporations; (4) firms that are required by law to maintain records of plain text communications or do so voluntarily; (5) firms that undergo an annual audit under general accounting principles; (6) strategic partners of United States corporations; and (7) on-line merchants who use encryption to secure electronic commercial transactions).

121. *See id.* Tit. V, sec. 504(a)(3) (permitting the export of encryption products pursuant to a license exception for encryption products sold or licensed to members of NATO, the OECD, and members of ASEAN).

122. *See* Statement by the White House Press Secretary, *Administration Announces New Approach to Encryption* (visited Sept. 20, 1999) <http://www.bxa.doc.gov/Encryption/whpr99.htm> (stating that the proposed reforms are based on three principles: (1) a one-time technical review of encryption products prior to their sale; (2) a streamlined post-export reporting system; and (3) a system that allows the United States government to review the export of encryption to foreign governments and military organizations and to blacklisted nations); *see also* Charles Bogino, *Administration Eases Encryption Curbs, Sends Congress Plan to Permit Key Recovery*, 16 Int'l Trade Rep. (BNA) No. 37, at 1510-11 (Sept. 22, 1999) (discussing the positive consequences of such liberalization for the law enforcement community, and Congress' reaction towards these proposed measures);

the regulations that United States encryption exporters deem overly burdensome by permitting the export of encryption commodities or software to businesses and other non-government end-users, and mass-market encryption commodities and software of any key length, pursuant to a one-time technical review.[123] Additionally, the Administration announced that it will implement the Cryptography Note, adopted by Wassenaar members in December 1998,[124] which will permit the unrestricted export of mass-market encryption commodities and software with key lengths of 64-bits or less.[125] Notwithstanding this announcement, congressional leaders remain skeptical that the Administration will follow through on its promise.[126]

In conjunction with the Administration's announcement, President Clinton sent a legislative proposal to Congress entitled the Cyberspace Electronic Security Act ("CESA"),[127] which provides law enforcement agencies with the necessary tools to combat the illegal

---

Statement of Rep. Bob Goodlatte on Today's Administration Encryption Export Policy Announcement (visited Sept. 27, 1999) <http://www.house.gov/apps/list/press/va06_ goodlatte/091699nr.html> (remarking that the announcement was a direct result of the SAFE Act's bipartisan support and noting that the proposed changes to United States encryption policy reflects many of the SAFE Act's key provisions).

123. *See* White House Fact Sheet, *Administration Announces New Approach to Encryption* (visited Sept. 20, 1999) <http://www.bxa.doc.gov/Encryption/whfs99.htm> (delineating the main components of the Administration's proposed update to its export control policy).

124. *See supra* notes 17-19 and accompanying text (outlining the substance of the December 1998 amendments to Wassenaar).

125. *See* Department of Commerce Press Release, *Clinton Administration Announces Major Easing of Encryption Export Controls* (visited Sept. 20, 1999) <http://www.bxa.doc.gov/Encryption/docpr99.htm> (discussing the proposed implementation of the December 1998 revisions to Wassenaar, which would decontrol the export of encryption items to all nations, except the seven sponsors of international terrorism, with key lengths of 64-bits or less).

126. *See* Bogino, *supra* note 122, at 1511 (stating that Senator John McCain, sponsor of the PROTECT Act, expressed skepticism that the encryption regulations would be significantly relaxed).

127. *See* Cyberspace Electronic Security Act of 1999 (visited Oct. 17, 1999) <http://www.cdt.org/crypto/CESA/CESArevised.shtml> (purporting to support the use of encryption, protect the security of encryption keys, and facilitate law enforcement's access to plain text for legitimate law enforcement purposes).

uses of encryption.[128] CESA authorizes the disclosure of encryption keys to recovery agents, their officers, employees or agents, to government agents, pursuant to a court order or search warrant.[129] Under CESA, a court would grant such an order upon finding that: the use of the recovery information is reasonably necessary to obtain the encrypted data, and such access is lawful, sought within a reasonable time, and does not infringe on any constitutionally protected privacy interests.[130] Another main element of the CESA is its proposed authorization of appropriations to the FBI of up to $80 million for a Technical Support Center that would serve to respond to the increasing use of encryption for criminal purposes.[131]

III. THE WASSENAAR ARRANGEMENT: AN INEFFECTIVE MULTILATERAL EXPORT CONTROL REGIME

Central to Wassenaar's ineffectiveness is its lack of an enforcement mechanism, thereby imposing no obligation on its signatories to enact domestic legislation consistent with its provisions.[132] Al-

---

128. *See Message to the Congress Transmitting the Proposed Cyberspace Electronic Security Act of 1999*, 35 WEEKLY COMP. PRES. DOC. 1760 (Sept. 16, 1999) (remarking that the CESA would limit the government's use and disclosure of encrypted information by requiring a court order or search warrant as a condition for obtaining such information, and would authorize appropriations for a Technical Support Center).

129. *See* Cyberspace Electronic Security Act of 1999, *supra* note 127, sec. 203 (proposing to amend sec. 2712(a) of Chapter 121 of Title 18, United States Code). In addition, sec. 2712 authorizes disclosure of encrypted data to government agents in emergency situations involving: (1) an immediate danger of death or serious physical injury to any person; (2) conspiratorial activities that threaten the national security of the United States; or (3) conspiratorial activities that are characteristic of organized crime or terrorism. *See id.*

130. *See id.* (providing the requirements for granting a court order for disclosure of recovery information under proposed sec. 2712(b)).

131. *See id.* sec. 207 (authorizing appropriations to the FBI for a Technical Support Center as follows: $25 million for fiscal year 2000, $20 million for fiscal year 2001; $20 million for fiscal year 2002; and $15 million for fiscal year 2003).

132. *See* Elec. Privacy Info. Ctr., *Cryptography and Liberty 1999: An Int'l Survey of Encryption Policy*, 11-12 (1999) (noting that Wassenaar is not a law or treaty but rather is designed primarily to foster the exchange of information); *see*

though COCOM was also a non-binding international agreement,[133] Wassenaar critics assert that The Arrangement has nowhere near "the discipline, the structure, and the coherence that [COCOM] had."[134] Wassenaar critics attribute the foregoing weakness to the increasingly liberal views of United States allies to technology transfers, and fears that the United States would dominate Wassenaar as it did COCOM.[135] An additional weakness is that several of the world's leading encryption-exporting nations[136] are not parties to The Arrangement.[137] Furthermore, Europe's leading Wassenaar members have begun to resist efforts by the United States to create a multilateral export control regime on United States terms and have, in this regard, started to deregulate their domestic export control laws.

A. 1998 AMENDMENTS TO WASSENAAR

In December 1998, Wassenaar members adopted amendments that placed a maximum 64-bit length on mass-market encryption ex-

---

also The Wassenaar Arrangement, *supra* note 1 and accompanying text (citing the Initial Elements of Wassenaar).

133. *See* Dursht, *supra* note 2, at 1100 (explaining that the enactment of domestic legislation was the only way COCOM's signatories could give its principles legal effect).

134. *Export Administration Act: Hearings on H.R. 361 Before the Subcomm. on International Economic Policy and Trade of the House Comm. on International Relations*, 105th Cong. 5 (1997) (statement of Paul Freedenberg, International Trade Consultant, Baker & Botts, L.L.P.) [hereinafter Freedenberg Statement] (alteration in original).

135. *See id.* (remarking that the United States' Wassenaar allies forced the Administration to accept a regulatory framework that is substantially weaker than COCOM). Freedenberg also observes that the single member veto that made COCOM so influential is missing in Wassenaar. *See id.* This veto prevented one member of COCOM from granting an export license for a certain product if another member vetoed that license following a review by a full committee. *See id.*

136. *See* Smith Statement, *supra* note 54 (remarking that China, India, Israel, and South Africa are absent among Wassenaar's members).

137. *See* Hoffman, *supra* note 20, at 47-51 (breaking down the numbers of encryption products all nations have developed including non-Wassenaar countries. India, Israel, and South Africa have reportedly developed 47 encryption products combined, for a 6% share of the global encryption market. *See id.*

ports.[138] Administration officials announced with great fanfare that the revisions would level the playing field among United States and foreign manufacturers of encryption products.[139] Without a binding enforcement mechanism and the lack of any implementation by the BXA, however, this amendment rings hollow for United States exporters;[140] the BXA still controls mass-market encryption commodities and software at the 56-bit level.[141] As a result, foreign encryption manufacturers will continue to develop more mass-market products and gain a stronger foothold in the global encryption market.

B. LITTLE INCENTIVE FOR COOPERATION

There is a danger that the combination of the lack of a common enemy[142] among Wassenaar partners, the varying degrees of economic development achieved by eastern European members,[143] and the need for those fledgling economies to establish new export markets may impede cooperation among Wassenaar members.[144] Given that Wassenaar does not require its signatories to notify each other

---

138. *See* The Wassenaar Arrangement, *supra* note 18, Category 5-pt. 2, at 613-17 (showing the revised Dual-Use Control List); Markoff, *supra* note 19, at A1 (discussing the Administration's reaction to revisions in Wassenaar); Yerkey, *supra* note 107, at 2046-47 (summarizing the 1998 amendments to Wassenaar).

139. *See* Markoff, *supra* note 19, at C4 (noting positive effects claimed by the Administration of the 1998 Wassenaar amendments on United States exporters).

140. *See* Gary G. Yerkey, *Administration Engaged in 'Burst of Activity' to Settle Int'l Encryption Export Dispute*, 15 Int'l Trade Rep. (BNA) No. 17, at 724-25 (Apr. 29, 1998) (summarizing both the reaction of the Administration and the technology industry to the Wassenaar amendment).

141. *See* 15 C.F.R. sec. 742.17 (1999) (setting forth the current BXA regulations governing mass-market encryption products).

142. *See* Dursht, *supra* note 2, at 1099 (commenting that the United States and its European allies established COCOM in response to fears of Soviet aggression and hostilities during the Berlin Crisis and the communist revolution in China).

143. *See* BAKER & HURST, *supra* note 1, at 72 (including, among the Eastern European members of Wassenaar, Bulgaria, the Czech Republic, Hungary, Poland, Romania, Russia, Slovakia, and Ukraine).

144. *See* Dursht, *supra* note 2, at 1116 (asserting that nations such as Bulgaria, the Czech Republic, Hungary, and Poland did not previously have export control laws under their command economies, and are, therefore, struggling to meet Wassenaar's requirements while trying to establish new markets for their exports).

when granting export licenses, members may easily grant export licenses to companies whose prior applications were denied by another member for the same export.[145] Additionally, Wassenaar's requirement that all decisions be reached by consensus may create less incentive for members to exchange information vital to controlling exports of sensitive dual-use technologies.[146] In sum, the lack of sufficient incentives for Wassenaar members to enact domestic policies consistent with The Arrangement's provisions will continue to prevent United States exporters from competing on the same level as their foreign counterparts.

C. INTANGIBLE EXPORT OF ENCRYPTION PRODUCTS

The lack of an enforcement mechanism frustrates efforts by United States exporters, who must abide by export laws that either mirror or are more restrictive than Wassenaar, to compete with foreign manufacturers in the global encryption market.[147] One outcome, as recent studies demonstrate, is that stringent United States laws have led to a significant increase in the amount of encryption products that are available from foreign manufacturers.[148] For instance, The Arrangement does not require members to control the intangi-

145. *See id.* at 1113 (contrasting the reporting requirements under Wassenaar with that of COCOM).

146. *See id.* (concluding that information exchanges are less likely to occur where it is well established that one member can prevent the adoption of certain proposals); *see also* Freedenberg Statement, *supra* note 134 (noting that since 1997, the United States government has been rather unsuccessful at convincing fellow signatories to participate in a reasonable level of exchange).

147. *See* Smith Statement, *supra* note 54 (remarking that the Administration has subjected United States exporters to more stringent regulations than those provided by Wassenaar). Smith also argues that in order to provide interim relief to United States firms, the Administration should raise the maximum exportable bit length to the 64-bit level provided for by Wassenaar. *See id.*

148. *See* Hoffman, *supra* note 20, at 6 (setting forth statistics evidencing a 149-product increase (22%) in the amount of encryption products available from foreign sources between December 1997 and May 1999). Newcomers to the manufacture and export of encryption products since December 1997 include Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey. *See id.* at 8. The study also provides a complete breakdown of the countries that are manufacturing encryption products. *See id.* at 7, Table 1.

ble[149] export of encryption software in cyberspace.[150] In the United States, however, current regulations restrict the distribution of encryption software via the Internet.[151] The foregoing has allowed software manufacturers from newly emerging countries to make their encryption software available over the Internet,[152] and establish a reputation for security that United States-exported products cannot match in foreign markets.

With respect to the intangible export of encryption products, United States Attorney General Janet Reno recently made overtures to Germany to work with the United States on the international distribution of such products.[153] Essentially, Ms. Reno argues that the

---

149. *See* BAKER & HURST, *supra* note 1, at 75 (including encryption software that can be downloaded off the Internet as an intangible export).

150. *See* Statements of Understanding and Validity Notes (last modified Dec. 3, 1998) <http://www.wassenaar.org/list/souval.pdf> (stating that Wassenaar members are expected to control the export of intangible technologies only so far as their domestic laws will allow); *see also* Elec. Privacy Info. Ctr., *supra* note 132, at 14 (characterizing the lack of controls on downloads of encryption products over the Internet as one of several loopholes).

151. *See* 15 C.F.R. sec. 734.2(b)(9)(ii) (describing Internet "exports" as including the downloading, or causing the downloading of, encrypted software to locations outside the United States or making such software available for transfer outside the United States, save Canada, over the Internet, unless the person making it available takes adequate precautions to prevent such "exports").

152. *See* SOLVEIG SINGLETON, ENCRYPTION POLICY FOR THE 21ST CENTURY: A FUTURE WITHOUT GOVERNMENT-PRESCRIBED KEY RECOVERY 22 (Cato Institute Policy Analysis No. 325, 1998) (providing as an example of the growth of foreign competition, South Africa-based Thawte Consulting, Inc., which manufactures software with 128-bit encryption that is distributed over the Internet). Singleton argues that the list of reputable products being distributed over the Internet "enables the creation of strong encryption products from weak products," and "fill[s] a gap in the market left by Internet browsers crippled by United States export controls." *Id.* at 23; *see also* Smith Statement, *supra* note 54 (noting that people living outside the United States can visit the international "Pretty Good Privacy" web site and download 128-bit encryption in less than one minute).

153. *See Reno Calls for Ban on Encryption Products on the Net*, Newsbytes PM, July 28, 1999, *available in* LEXIS, News Library, Asapii File (remarking that the liberal distribution of encryption products over the Internet will render Wassenaar controls useless). In a letter to German Federal Secretary of Justice Herta Daubler-Gmelin, Reno stated:

global proliferation of encryption software that is downloadable from the Internet will render Wassenaar useless in controlling such encryption exports.[154] Representatives of both the German government and business community responded by suggesting that Wassenaar was not designed to inhibit "bona-fide civilian transactions,"[155] and that regulation of the Internet distribution of encryption products runs counter to Germany's domestic policy, which is based on the "free availability of encryption products."[156] This statement is indicative of the way in which Wassenaar members loosely interpret The Arrangement's provisions.

D. EUROPEAN LIBERALIZATION TRENDS

COCOM's dissolution in 1994 and the intensification of the encryption debate signaled to the Administration that it could no longer maintain its current export policy without broad international support.[157] Hence, the United States attempted to use its global leader-

---

> [S]ome Wassenaar Nations continue not to control encryption software that is distributed over the Internet, either because the software is in the "public domain" or because those Nations do not control distribution of intangible items . . . unless we address this situation, use of the Internet to distribute encryption products will render Wassenaar's controls immaterial.

See id.; *see also* Letter from Janet Reno, United States Attorney General to Herta Daubler-Gmelin, Federal Secretary of Justice (May 1999) (last modified July 29, 1999) <http://www.heise.de/tp/english/inhalt/te/5124/2.html>.

154. *See Reno Calls for Ban on Encryption Products on the Net*, *supra* note 153 (observing that the enactment of Reno's proposal would signal the end of Internet distribution of encryption products, including highly popular web browsers such as Netscape).

155. *See id.* (quoting Thomas Roessler, spokesperson of Germany's *Foerdervereins* Information Technology and Society). Roessler further views Reno's efforts as an extension of the United States' desire to maintain its electronic surveillance capabilities. *See id.*

156. *See id.* (quoting Hubertus Soquat, an adviser in the German Federal Ministry for Economic Affairs).

157. *See* Stewart A. Baker, *Decoding OECD Guidelines for Cryptography Policy*, 31 INT'L LAW. 729 (1997). Stewart Baker, formerly the General Counsel for the National Security Agency, participated as a member of the United States delegation to the OECD negotiations. *See id.* In particular, he participated in the drafting process led by the United States Council for International Business. *See id.*

ship position to press the OECD[158] to author guidelines on encryption that reflected current United States export laws and adopted the Administration's key recovery proposals.[159] In the end, however, the OECD guidelines dealt a major blow to the United States and its efforts to create a global export control system on encryption that endorsed key recovery.[160] Without broad international support, the United States has seen its main allies[161] in this battle retreat from promoting key recovery in their own countries.[162]

---

158. *See* BAKER & HURST, *supra* note 1, at 42 (outlining the structure and purposes of the OECD). The OECD is an intergovernmental organization that was formed in 1961 as the successor for the Organization for European Economic Cooperation, which was established to help administer the Marshall Plan that rebuilt post-World War II Europe. *See id.* The OECD's 29 members include Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, The Netherlands, New Zealand, Norway, Poland, Portugal, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. *See id.*; *see also* SCOTT SULLIVAN, FROM WAR TO WEALTH: FIFTY YEARS OF INNOVATION 6 (1998) (describing the OECD as a meeting place for developed capitalist nations to promote such diverse policy concepts as export credits, corporate governance, and the control of the dissemination of Internet pornography).

159. *See* Elec. Privacy Info. Ctr., *supra* note 132, at 15 (using a delegation led by the DOJ, FBI, and the National Security Agency, the United States lobbied before the OECD for an international key escrow policy); Markoff, *supra* note 19, at A1 (commenting that no consensus existed among the various delegations); *see also* Baker, *supra* note 157, at 736 (analyzing Principle Six of the OECD guidelines as the only principle in the guidelines that does not make a recommendation to member governments, but only states that governments may adopt key recovery schemes).

160. *See* Markoff, *supra* note 19, at A1 (commenting on the OECD's rejection of a United States proposal to endorse the use of key recovery on a global scale).

161. *See* discussion *infra* Part III.D (analyzing the encryption policies of the European Union, France, Germany, and the United Kingdom).

162. *See France Heralds Fall of its Crypto 'Maginot Line,'* COMMUNICATIONS WEEK INTERNATIONAL, Feb. 1, 1999, *available in* 1999 WL 11859264 (summarizing the key aspects of France's new encryption policy as compared to its 1996 law); *UK Government Abandons Plans for Tougher Regulation of Internet Commerce*, AFX NEWS, May 26, 1999, *available in* LEXIS, News Library, Extafx File (announcing that the United Kingdom government removed from pending electronic commerce legislation a requirement that encryption users leave copies of their decoding keys with escrow agents or the police).

1. The European Union

European Union[163] controls on encryption exports are governed by the Council of the European Union's[164] Decision[165] on the control of exports of dual-use goods ("EU Dual-Use Decision").[166] With respect to encryption, the European Union recently began promoting the development of a common encryption policy.[167] In October, 1997, the European Commission[168] published its Communication[169] on encryp-

---

163. *See generally* EU COMMITTEE OF THE AMERICAN CHAMBER OF COMMERCE, EU INFO. HANDBOOK 5-12 (1997) (discussing the history, structure, and functioning of the European Union and its main policy-making organs); IAN BARNES & PAMELA M. BARNES, THE ENLARGED EUROPEAN UNION 7-50 (1995) (presenting a detailed description of the functions of the various European Union institutions).

164. *See* EU COMMITTEE OF THE AMERICAN CHAMBER OF COMMERCE, *supra* note 163, at 117 (noting that the main function of the Council of the European Union is to adopt legislation that various arms of the European Union have proposed, and likening this function to that of a parliamentary body).

165. *See id.* at 9 (defining a decision as a legislative act that is issued by the Council of the European Union or the European Commission, and is binding upon those member states to which it is addressed).

166. *See* Council Decision 94/942/CFSP, General Software Note, 1994 O.J. (L 367) (outlining the types of software that the European Union excludes from export controls).

167. *See Towards a European Framework for Digital Signatures and Encryption* (visited Sept. 26, 1999) <http://www.ispo.cec.be/eif.policy/97503.html> (setting forth the European Commission's proposal for developing a union-wide encryption policy). Prior to the Commission's release of the proposal to the European Parliament, The Council, the Economic and Social Committee, and the Committee of the Regions, the ministers of 29 European nations gathered in Bonn, Germany, at the Global Information Networks Ministerial Conference, held July 6-8, 1997, to discuss the development of a pan-European and worldwide information technology policy. *See Industrial Declaration* (visited May 27, 1999) <http://www.echo.lu/bonn/industry.html>; *see also* Arthur Rogers, *EU Parliament Urges Members to Back Unified Export Control Policy*, 16 Int'l Trade Rep. (BNA) No. 16, at 662-63 (Apr. 16, 1999) (announcing the European Parliament's call for member nations to drop their opposition to a common export control policy for dual-use goods).

168. *See* EU COMMITTEE OF THE AMERICAN CHAMBER OF COMMERCE, *supra* note 163, at 17 (setting forth the functions of the European Commission, which include, *inter alia*, the introduction of legislation and ensuring that the provisions of the Treaty on European Union are correctly applied). The Treaty on European Union assigns to the Commission several responsibilities, including those of "supervision, initiative and implementation." *See id.*

tion, which rejected the United States' position on key escrow and sought to implement regulations that address the privacy and business needs of Europeans.[170] As a corollary to the Communication, the European Parliament called on its member states to advocate that the Wassenaar list of "encryption products subject to export restrictions be reduced to a *strict minimum* and that, consequently, no new restrictions should be introduced."[171] One sign of the distrust regarding United States key recovery initiatives is the European Parliament's[172] recent release of a report accusing the National Security Agency ("NSA") of spying on European companies after learning that the NSA held the keys to certain United States-made software used by such companies.[173]

---

169. *See id.* at 9-10 (characterizing a Communication as a document normally released pursuant to comments on a Green Paper, which is a consultative document that provides information on a specific issue for which legislation has not been enacted, and may provide an outline for future Commission legislative proposals).

170. *See Towards a European Framework for Digital Signatures and Encryption*, *supra* note 167, at 2.2(ii) (outlining the rationale behind the European Commission's rejection of key escrow). According to the European Commission, regulations attempting to restrict the use of encryption will be ineffective because the Internet provides easy access to encryption software by allowing persons to download the software. *See id.* Additionally, it is difficult to identify users of encryption software. *See id.* Furthermore, messages can be encrypted within other data in a way that the existence of an encrypted message cannot be detected. *See id.* Consequently, regulations on the use of encryption would prevent law-abiding citizens and companies from protecting themselves against criminal attacks. *See id.* The Commission drafted the Communication partly because it felt that the current dual-use regulations, enacted by the European Council in 1994, regulated encryption exports between member states as much as it regulated exports outside the European Union. *See* Rogers, *supra* note 167, at 662. Additionally, the current dual-use regulations did not appropriately specify the scope of national controls required to adhere to the regulation. *See id.*

171. Commission Resolution, 1998 O.J. (C 292) (emphasis added).

172. *See* EU COMMITTEE OF THE AMERICAN CHAMBER OF COMMERCE, *supra* note 163, at 141 (commenting that the European Parliament, which is elected by universal suffrage, functions as the direct representative of European citizens and holds the power to veto legislation in certain areas).

173. *See* Ann Harrison, *Report Says U.S. Has Backdoor to Notes: European Body Levels Charge, Warns Users*, COMPUTERWORLD, May 31, 1999, *available in* LEXIS, News Library, Cmpwld File (reporting that a new European Parliament report charges that the United States National Security Agency is able to access

At the time of the Communication's publication, member states such as France and the United Kingdom opposed a common encryption policy.[174] Recent reforms by these two nations, however, have made the creation of a common European Union policy more realistic.[175] Such reforms, which include the abandonment of mandatory key recovery,[176] will further frustrate the Administration's efforts to strengthen Wassenaar with a key recovery provision. Furthermore, United States exporters will suffer greater economic harm as more United States trading partners will find new markets for their encryption exports.[177]

2. *France*

Until recently, France had the most stringent encryption laws among nations regulating encryption products.[178] At the time the OECD published its guidelines, France supported the United States effort to create a multinational export control regime that mandated

---

data from export versions of Lotus Notes software). The report accurately states that 24-bits of the 64-bit version of Lotus Notes are "encrypted in a public key supplied by the United States government that is buried in the user's Notes software." *Id.*; *see also* Aucsmith Statement, *supra* note 46 (observing that the maker of Lotus Notes lost a large sale to the Government of Sweden when the Swedish press reported that the software had a key recovery feature).

174. *See* BAKER & HURST, *supra* note 1, at 122 (stating that the Communication's viewpoints differ sharply from those espoused by the United States, France and the United Kingdom).

175. *See* discussion *infra* Part III.D (discussing the recent moves towards liberalization by France, and the United Kingdom).

176. *See France Heralds Fall of its Crypto 'Maginot Line,' supra* note 162; *UK Government Abandons Plans for Tougher Regulation of Internet Commerce, supra* note 153 (providing reasons why the UK government discarded its mandatory key recovery proposal in recent electronic commerce legislation).

177. *See* Strassel, *supra* note 47, at 1 (commenting that foreign software manufacturers have used their encryption products to sell other non-encrypted software and further damage the economic interests United States software manufacturers).

178. *See* Elec. Privacy Info. Ctr., *supra* note 132, at 50 (commenting that until early 1999, France maintained a complex licensing scheme for the import and domestic use of encryption products); BAKER & HURST, *supra* note 1, at 130 (remarking that the French government's strict regulations on encryption exports originate from the French view that technology and industrial policy play a vital role in its national defense).

governmental use of key recovery.[179] France's 1998 decree, which implemented Article 17 of France's Law on Telecommunications Regulations of 1996,[180] tightly regulated the use of encryption products for domestic and external consumption.[181] Although the 1996 Law did not restrict the use of encryption for uses that protected the confidentiality of data, France's encryption regulations remained stricter than Wassenaar.[182] Thus, the Administration assumed that it could rely on France for support of its agenda to control encryption exports on a global level.

On January 19, 1999, French Prime Minister Lionel Jospin announced a significant change in France's encryption policy, pursuant to which the domestic encryption threshold would increase from 40-bits to 128-bits.[183] Among the changes,[184] the French government af-

---

179. *See generally* Markoff, *supra* note 19; *see also* Baker, *supra* note 157, at 731 (observing that the French government restricts the domestic use of encryption products, and requires encryption users to obtain prior government authorization).

180. *See* BAKER & HURST, *supra* note 1, at 132 (providing a brief summary of Article 17 as adopted on July 26, 1996).

181. *See id.* (stating that French law created varying export regulations for different types of encryption technologies). The 1998 decrees categorized encryption products by: (1) deregulating the use of encryption items that were incapable of securing the confidentiality of data, including "encryption used to authenticate a communication, digital signature technologies and access control functions," however, exporters are still required to submit a "declaration" to the *Service Central de la Sécurité des Systèmes d'Information* ("SCSSI") one month prior to exporting the product; (2) liberalizing the domestic use of encryption products whose keys are entrusted to a government-approved key recovery agent, however, France still controls the export of such products; and (3) requiring all remaining encryption products not governed by the other two categories to require prior authorization from the SCSSI. *See id.* at 132-33.

182. *See id.* at 132 (explaining that requiring prior government approval for the export of encryption items does not protect the confidentiality of data).

183. *See* Elec. Privacy Info. Ctr., *supra* note 132, at 51 (summarizing the encryption policy reforms in France); *France Heralds Fall of its Crypto 'Maginot Line'*, *supra* note 162 (observing that the new policy is partially the result of intense lobbying by 200 French companies, multinationals, and trade associations led by the French Association of Unix Users); *see also France Allows 128-bit Crypto* (visited Aug. 6, 1999) <http://jya.com/fr-128bit.htm> (translating an excerpt from the Prime Minister's announcement concerning France's new encryption policy).

184. *See* Elec. Privacy Info. Ctr., *supra* note 132, at 50-51 (outlining the ration-

firmed its commitment to Wassenaar by proposing export controls on encryption products using 56- or 64-bit length encryption.[185] This marks a significant increase from previous regulations that restricted the export of encryption products with greater than 40-bit length encryption capabilities.[186] Proponents of United States export laws and Wassenaar argue that France's reforms are insignificant in the global context because the government still maintains export controls at Wassenaar levels.[187] Nonetheless, France's abandonment of mandatory key recovery indicates a fracture in its alliance with the United States, and thereby damages United States efforts to strengthen Wassenaar with global key recovery standards.[188]

---

ale behind and the proposed changes to current French encryption laws). Domestically, the new law would eliminate the need for encryption users to place keys with government-approved key recovery agents and would allow the internal use of encryption as strong as 128-bits, replacing the old ceiling of 40-bits. *See id.* Prime Minister Jospin remarked that the changes were needed in part to prevent France's possible isolation from its main trading partners. *See id.*; *see also France Heralds Fall of its Crypto 'Maginot Line'*, *supra* note 162 (stating that French officials justified the need for the new policy in order to address concerns over industrial espionage by trading partners and their commercial adversaries).

185. *See France Heralds Fall of its Crypto 'Maginot Line'*, *supra* note 162 (remarking that France will continue to respect its international commitments under Wassenaar by maintaining export controls on encryption products with more than 64-bit encryption); *see also* Elec. Privacy Info. Ctr., *supra* note 132, at 51 (describing the provisions of the draft bill that will be sent to the French Parliament). According to this survey, the draft bill contains a provision that maintains export controls on encryption products with over 56-bit length encryption. *See id.*

186. *See* BAKER & HURST, *supra* note 1, at 131 (discussing the previous French encryption policy).

187. *See Encryption and Export Security: Hearings on H.R. 850 Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (1999), *available in* 1999 WL 503725 (statement of Congressman Porter J. Goss, Chairman, House Permanent Select Comm. on Intelligence) (remarking that although France has proposed significant reforms in domestic encryption policy, the government maintains restrictions on exports consistent with Wassenaar).

188. *See Online Encryption Technology: Hearings Before the Subcomm. on Communications of the Senate Comm. on Commerce*, 105th Cong. (1997), *available in* 1999 WL 136078 (statement of Ambassador David L. Aaron, United States Special Envoy for Cryptography) (remarking that his goal as special envoy for cryptography is to develop an international consensus in favor of global key recovery systems).

3. Germany

Unlike France, Germany's encryption export policy is not governed by one specific law, but is modeled after the EU Dual-Use Decision.[189] Germany, also a Wassenaar member, has vigorously opposed restrictions on the use and export of encryption products for two reasons.[190] First, the German government finds that encryption is underutilized by German society,[191] and it is, therefore, encouraging German manufacturers to produce encryption products for both domestic and external use.[192] In effect, Germany's need for greater security makes it wary of United States-manufactured products, which some members of the German Parliament believe are tampered with by the NSA. Second, the German government views encryption as an important element in crime prevention,[193] although it recognizes that the user-friendly nature of encryption may lead to increased use among criminals.[194] To that end, the German government's federal agencies[195] will continue to monitor the spread of encryption to en-

---

189. *See* Chrisopher Kruner, *Cryptography Regulation in Germany, reprinted in* BAKER & HURST, *supra* note 1, at 151-52 (stating that the EU Dual-Use Decision is one of the main legal instruments by which the German government regulates the export of encryption products).

190. *See* Elec. Privacy Info. Ctr., *supra* note 132, at 53 (describing Germany as one of the staunchest opponents of restrictions on encryption, playing a significant role in preventing key escrow provisions from being inserted into Wassenaar).

191. *See Key Elements of Germany's Encryption Policy*, (visited Aug. 6, 1999) <http://jya.com/de-crypto-all.htm> (explaining that encryption is not utilized to the extent it should be because of a lack of consciousness regarding technology security).

192. *See id.* (decreeing that Germany has vital business and security interests in promoting the use of encryption).

193. *See id.* (noting that the government's ability to guarantee the confidentiality of data will lead to improved crime prevention). The government recognizes, however, that the future may bring increased use of encryption to conceal criminal activity. *See id.* German law enforcement authorities are, therefore, committed to ensuring that judicially-approved surveillance tactics remain effective. *See id.*; Christopher Kuner, *Cryptography Regulation in Germany, in* BAKER & HURST, *supra* note 1, at 157.

194. *See Key Elements of Germany's Encryption Policy*, *supra* note 191 (recognizing the potential for misuse and abuse of encryption for illicit activities).

195. *See* Kuner, *supra* note 193, at 151 (noting that the *Bundesamt für Sicherheit*

sure that it does not adversely impact its surveillance capabilities.[196]

Germany's genuine concern for crime prevention did not prevent it from opposing United States efforts to place a mandatory key escrow provision in Wassenaar.[197] Largely influenced by the ongoing debate in the United States, German opposition to placing a mandatory key escrow provision in Wassenaar hinges upon an awareness of the tremendous costs associated with such a policy.[198] According to the German government, its financial resources would be better spent by enacting policies that will enhance the international competitiveness of German software firms.[199] As a result, German software manufacturers, most notably Brokat Information Systems AG,[200] have flourished and gained a strong foothold in the global encryption market.

4. United Kingdom

The United Kingdom, which also enacted export controls over encryption products consistent with Wassenaar,[201] had until recently joined France and the United States in lobbying the OECD to man-

---

in der Informationstechnik ("BSI") is the leading government agency concerned with encryption and is an offshoot of the German foreign intelligence service).

196. *See Key Elements of Germany's Encryption Policy*, *supra* note 191 (naming this objective as one of the five key elements of Germany's encryption policy).

197. *See* Elec. Privacy Info. Ctr., *supra* note 132, at 53 (explaining that in 1999, German efforts prevented the inclusion of key escrow provisions in Wassenaar).

198. *See* Kuner, *supra* note 193, at 166 (asserting that like most members of Wassenaar, the German government desires a cost-effective encryption policy that will effectively hinder the criminal use of encryption).

199. *See id.* (noting that the fierce encryption debate in the United States gives Germany an opportunity to capitalize on the competitive advantage liberal German encryption policy provides).

200. *See supra* note 51 for a discussion on the success enjoyed by *Brokat* Information Systems AG, a German software manufacturer that has capitalized on the heavy-handed United States export controls.

201. *See* Henry Beker & Chris Emery, *Cryptography Policy—The United Kingdom Perspective*, *in* BAKER & HURST, *supra* note 1, at 233 (stating that the United Kingdom follows Wassenaar). In a 1997 paper entitled *Licensing of Trusted Third Parties for the Provision of Encryption Services*, the United Kingdom's Department of Trade and Industry indicated that it would pursue a key escrow initiative. *See id.* at 237.

date the international acceptance and development of international key recovery systems.[202] British encryption policy is governed by its Dual-Use and Related Goods (Export Control) Regulations of 1996.[203] Interestingly, however, the United Kingdom lacks control over encryption software that is tangible,[204] generally available,[205] or in the public domain.[206] This is due to the United Kingdom's implementation of the European Union's General Software Note,[207] part of the EU Dual-Use Decision, which exempts such software from export controls.[208]

In May 1999, the United Kingdom government abandoned attempts to insert mandatory key recovery provisions into electronic commerce legislation.[209] Prime Minister Tony Blair cited the United

---

202. *See* Elec. Privacy Info. Ctr., *supra* note 132, at 99 (observing that the United Kingdom had been the strongest supporter of United States efforts to promote key recovery, as evidenced by its joining the United States in attempting to influence the OECD to require governments to adopt mandatory key recovery in their domestic policies).

203. Dual-Use and Related Goods (Export Control) Regulations of 1996, S.I. 1996, No. 2721.

204. *See id.* (defining software as "one or more programmes or microprogrammes fixed in any *tangible* medium of expression") (emphasis added).

205. *See* BAKER & HURST, *supra* note 1, at 223 (mirroring the European Union's General Software Note, which defines "generally available" software as that sold by retailers via over-the-counter transactions or mail and telephone order transactions).

206. *See id.* (adopting European Union regulations, which define "public domain" software or technology as that which is available without limitations on its subsequent distribution). Like the European Union, copyright restrictions do not remove software from the public domain category in the United Kingdom. *See id. But see* Security and Freedom Through Encryption (SAFE) Act, H.R. 850, 106th Cong. sec. 3(a) (1999) (purporting to decontrol export controls on encryption software or hardware that is in the public domain for which copyright protection is not available under United States law).

207. Council Decision 94/942/CFSP, Gen. Software Note, 1994 O.J. (L 367).

208. *See id.* (exempting from control encryption software that is tangible, generally available, or in the public domain).

209. *See* Performance and Innovation Unit, *Encryption and Law Enforcement*, May 1999, at 13 (determining that after a careful assessment, the British government should reform its encryption policy because it could not meet its dual objec-

Kingdom's desire "to participate fully in the electronic revolution."[210] His motivations are reflected in a report recently published by the Performance and Innovation Unit ("PIU"), an advisory committee of the British government.[211] The PIU report concludes that the United Kingdom government has determined that the "implementation of mandatory key escrow would significantly impair the ability of the UK to become the leading environment in the world in which to trade electronically[.]"[212] Alternatively, British officials proposed the creation of a 24-hour technical assistance center, which, similar to the current Administration proposal,[213] would be established to decrypt lawfully intercepted data.[214]

IV. RECOMMENDATIONS FOR FURTHER LIBERALIZATION OF EXPORT CONROLS ON ENCRYPTION PRODUCTS

The EU's movement away from regulating encryption exports, and recent reforms to French, British and German encryption policies, demonstrate that current United States controls on

---

tives of becoming an e-commerce power and serving law enforcement needs); *see also UK Government Abandons Plans for Tougher Regulation of Internet Commerce*, *supra* note 162 (stating that the government's original plan would have required encryption users to deposit a copy of their decryption keys with the police or another third party).

210. *See UK Government Abandons Plans for Tougher Regulation of Internet Commerce*, *supra* note 162 (suggesting that the United Kingdom government based its decision to abandon mandatory key recovery on the international community's recent shift away from strict regulation of the Internet).

211. *See* Performance and Innovation Unit, *supra* note 209, at 17 (providing a brief history of and purpose behind the establishment of the PIU). The PIU's main goal is to "improve the capacity of government to address strategic, cross-cutting issues and promote innovation in the development of policy and in the delivery of government objectives." *See id.*

212. *Id.* at 13.

213. *See also supra* note 131 and accompanying text (proposing the creation and funding of a technical support center within the FBI).

214. *Compare id.* (explaining that a technical assistance center would serve as an effective alternative to mandatory key escrow, which would be used primarily as an intelligence gathering device), *with* Reno Statement, *supra* note 48 (characterizing the funding of a technical support center in the United States as essential to protecting the public safety).

encryption exports, which either mirror or are more restrictive than Wassenaar, are outdated and do not reflect market realities. While the Administration has proposed significant changes to the current encryption policy, the extent of the proposed liberalization is unknowable until December 15, 1999, the date by which such proposals are to be implemented. To remedy the economic harm that Wassenaar and domestic policy have perpetrated on United States encryption exporters, this Comment makes several recommendations that are set forth below.

A. A BINDING AND MORE INCLUSIVE MULTILATERAL EXPORT CONTROL REGIME

Conceptually, Wassenaar is an excellent means for controlling the proliferation of sensitive technologies such as encryption outside the developed world and, more importantly, to pariah nations. An enforcement problem arises, however, because The Arrangement is non-binding. Unlike COCOM, the lack of a common enemy provides little incentive for Wassenaar members to voluntarily comply with its encryption export control provisions.[215] Additionally, the thirty-three nations comprising the signatories to The Arrangement do not include some of the more prevalent exporters of encryption products.[216] Admittedly, international cooperation on the export of sensitive technologies may be an effective way of preventing their proliferation. However, a more inclusive and enforceable export control regime built on the existing Arrangement is necessary to achieve this end. Otherwise, there will continue to exist few inducements to comply with Wassenaar's principles.[217]

---

215. *See* discussion *supra* Part III.B (discussing the problems with voluntary compliance and its potential adverse effects on Wassenaar's effectiveness).

216. *See supra* notes 136, 137 (noting that Wassenaar does not include encryption exporting nations such as China, India, Israel, and South Africa); Elec. Privacy Info. Ctr., *supra* note 132, at 11-12 (including Estonia, Hong Kong, Iceland, India, and Mexico, which incidentally are not parties to Wassenaar, as encryption exporting nations or territories).

217. *See* Dursht, *supra* note 2, at 1090 (suggesting that group cooperative behavior relies on oversight and control mechanisms, and a sense among members of the group that the group interest is more important than the individual interest).

B. INCREASING THE ENCRYPTION THRESHOLD IN THE DUAL-USE CONTROL LIST TO AT LEAST 128-BITS

In conjunction with the creation of a binding international export control regime, the United States and its fellow Wassenaar members should revise the Dual-Use Control List to increase the exportable encryption threshold to at least 128-bits.[218] First, the current worldwide encryption standard is 128-bits,[219] and it is well documented that even 128-bit encryption is breakable.[220] Moreover, 128-bit encryption can be easily downloaded off the Internet in less than one minute.[221] Second, several leading Wassenaar members, such as France, Germany and the United Kingdom, have deregulated their export control regimes and are actively promoting the further development of their technology sectors.[222] As a result, encryption manufacturers from such nations are developing and exporting reliable 128-bit level en-

---

218. *See* Hornstein Statement, *supra* note 50 (commenting that the Administration's sectoral liberalization in 1998 did not go far enough because 128-bit encryption is the minimum required for current Internet applications). Hornstein also testified that the most popular encryption program, "Pretty Good Privacy," uses an encryption algorithm with a 128-bit key. *See id.*; *see also* Hoffman, *supra* note 20, at 6 (observing that at least 123 of the reported 805 foreign-made encryption products contain a bit length between 112 and 168-bits); Singleton, *supra* note 152, at 5 (providing statistics that there are currently 3.5 million users of "Pretty Good Privacy" worldwide).

219. *See* Black Statement, *supra* note 50 (commenting that the current standard for most encryption users is 128-bits, which is almost five sextillion times stronger than 56-bit level encryption).

220. *See id.* (noting that recent advances in decryption have illustrated the vulnerability of 128-bit level encryption); *see also* Hornstein Statement, *supra* note 50 (relating as an example of developments in speeding up decryption time, Israeli scientist Adii Shamir and his "Twinkle" computer); Singleton, *supra* note 152, at 7 (providing examples regarding the vulnerability of 56-bit level encryption). For instance, in July 1998, two cryptographers cracked the 56-bit code in 56 hours, using a single personal computer costing $250,000. *See id.* Although the author admits that 56-bit encryption sufficiently prevents most "casual hackers" from cracking the code, the market no longer trusts this level of technology." *See id.*

221. *See* Smith Statement, *supra* note 54 (observing that anyone in the world can download "Pretty Good Privacy" from its international web site within 47 seconds).

222. *See* discussion *supra* Part III.D.

cryption,[223] placing United States exporters at a competitive disadvantage. Third, the President's Export Council Subcommittee on Encryption recently recommended that the United States government permit the unrestricted export of mass-market encryption with key lengths of up to 128-bits.[224] To keep pace with technological advances, Wassenaar members should undertake a biannual review of the worldwide encryption standard,[225] pursuant to which members would revise the Dual-Use Control List and increase the level of freely exportable encryption to meet the current standard.

C. LEGISLATIVE SOLUTIONS TO ASSIST UNITED STATES EXPORTERS

In the short term, the United States should offset any future adverse effects to its technology industry by enacting the SAFE Act, which permits the unrestricted export of mass-market encryption products and bars the imposition of mandatory key recovery.[226] Current United States policy that permits the export of products with unlimited encryption strength to the banking, financial services, and health and medical sectors, on-line merchants, and international subsidiaries of United States companies, does not go far enough;[227] nor do proposals that recommend a sectoral, multi-tiered approach whereby the levels of encryption would fluctuate depending on the entity using it.[228] Rather, the SAFE Act provides a more flexible ap-

---

223. *See* Hoffman, *supra* note 20, at 6 (discussing the countries that are manufacturing strong encryption with 128-bits or higher).

224. *See* President's Export Council Subcommittee on Encryption, *Liberalization 2000: Recommendations for Revising the Encryption Export Regulations*, August 1999, at 3 (recommending that the Administration increase the maximum bit length for freely exportable encryption to 128 bits).

225. *See* Singleton, *supra* note 152, at 7 (observing that the power of a computer microprocessor doubles almost every 18 months).

226. *See* discussion *supra* Part II.C.1 (summarizing the key provisions to the SAFE Act).

227. *See* discussion *supra* Part II.B (discussing the most recent change in policy by the Administration, which permits the export of products with unlimited encryption to certain industrial sectors).

228. *See* Haignere, *supra* note 55, at 354-57 (recommending a three-tier approach to controlling encryption exports). According to the author, the United States would best be served by an approach that permits the export of the strongest

proach by permitting United States exporters to benefit from deregulation while maintaining the President's authority to restrict exports to those embargoed nations characterized as sponsors of worldwide terrorism.[229] Moreover, SAFE does not implicate national security because the products that SAFE decontrols are already available in foreign markets.[230]

D. IMPLEMENTATION OF THE ADMINISTRATION'S SEPTEMBER 1999 ENCRYPTION POLICY PROPOSAL

The full implementation of the Administration's recent proposals to decontrol the export of encryption commodities and software would constitute a drastic change in United States encryption policy. Easing such restrictions under the Administration's plan may preempt the need to enact the SAFE Act.[231] No longer would liberal encryption policies only benefit on-line merchants, banks and financial institutions, health and medical institutions, and foreign subsidiaries of United States companies.[232] Rather, liberal treatment would also

---

encryption to financial, medical, and insurance companies, followed by 96-bit level encryption for international use by private industry, and ending with 56-bit level encryption for mass-market communications mediums such as telephones, faxes, and e-mail. *See id.*

229. *See* Security and Freedom Through Encryption (SAFE) Act, H.R. 850, 106th Cong. sec. 3(c)(1)(A-B) (1999) (setting forth the President's power to limit encryption exports under SAFE); *cf.* Letter from Stewart A. Baker, Steptoe & Johnson, to Nancy Crowe, Regulatory Policy Division, Bureau of Export Administration (Mar. 1, 1999) (on file with the Bureau of Export Admin.) (recommending that the BXA revise the country list to exclude only the seven terrorist supporting nations from the country list for license exceptions under the September 1998 sectoral liberalization).

230. *See Armed Services OKs Weakened Encryption Export Bill*, CongressDaily, July 22, 1999, *available in* LEXIS, News Library, Cngdly File (arguing that the amendment to SAFE would do little to protect United States national security because strong encryption is widely available).

231. *See* Bogino, *supra* note 122, at 1511 (noting House Minority Leader Richard Gephardt's opinion that the Administration's proposal may preempt the need to enact the SAFE Act).

232. *See supra* notes 89-92 and accompanying text (detailing the new BXA regulations affecting exports of encryption products to banks and financial institutions, on-line merchants, hospitals and medical institutions, and United States subsidiaries overseas).

extend to mass-market encryption commodities and software,[233] permitting United States encryption manufacturers to sell products with the same level of security to both domestic and foreign consumers.

E. ABANDONING INTERNATIONAL KEY RECOVERY

The Administration's efforts to gain an international consensus on key recovery have all but collapsed, as countries that previously supported it have relented and realized the need to develop electronic commerce and to find new markets for their technology products.[234] In addition, the European Union continues to promote a common encryption policy that excludes mandatory key recovery.[235] Apart from the trend away from mandatory key recovery, an international key recovery regime is unrealistic because it would require a great deal of government coordination and a means for a foreign government to obtain decryption keys from a foreign escrow agent.[236] Hence, instead of imposing key recovery where no potential for cooperation or demand exists,[237] the United States should work with its technology industry and foreign governments to create less invasive solutions.

One such proposal involves the creation of a technical assistance center, as recently proposed by both the Administration and the United Kingdom's government.[238] In the United Kingdom, the tech-

---

233. *See* White House Fact Sheet, *supra* note 123 (proposing to permit the export of mass-market encryption commodities and software of any key length pursuant to a one-time technical review by the BXA).

234. *See* discussion *supra* Parts III.D.2., III.D.3 (discussing the recent rejection of mandatory key recovery by France and the United Kingdom)

235. *See supra* notes 163-73 (stressing that the European Union has opposed United States efforts to impose a global key recovery standard since the publication of the OECD's guidelines).

236. *See* Haignere, *supra* note 55, at 353 (finding unrealistic the possibility of creating an international key escrow system).

237. *See generally* Aucsmith Statement, *supra* note 46 (testifying that because of technical inefficiencies neither businesses nor consumers have a need for key recovery, especially for plain text access). In addition, Aucsmith testified that plain text access does not meet law enforcement or national security needs because law enforcement cannot verify compliance with key recovery requirements. *See id.*

238. *See supra* notes 213, 214 and accompanying text (comparing proposals by the United States and the United Kingdom for technical assistance centers that

nical assistance center would assist law enforcement agencies in intercepting encrypted communications to the extent permitted under United Kingdom law.[239] Similarly, the Administration's recent proposal under CESA would provide law enforcement agents access to decryption keys pursuant to a court order.[240] While this does not completely abandon key recovery, law enforcement would have indirect rather than direct access to encrypted communications. Decryption keys would no longer be held by government-affiliated escrow agents. Instead, law enforcement officials in both the United States and the United Kingdom would only gain access to decryption keys pursuant to proper judicial or governmental authorization.[241]

CONCLUSION

United States-led efforts to control the export of strong encryption, both through Wassenaar and domestic law, is neither a commercially viable nor realistic strategy. First, Wassenaar is non-binding and, therefore, merely serves as a guidepost for the development of an international export control regime. Second, recent reforms by European Wassenaar members demonstrate that Wassenaar is only as strong as its signatories choose it to be. For instance, Germany and

---

would assist law enforcement officials in decrypting data).

239. *See* Performance and Innovation Unit, *supra* note 209, at 7 (discussing the United Kingdom's Interception of Communications Act of 1985 ("IOCA"), which permits the interception of any communication transmitted over a public network pursuant to a warrant signed by the Secretary of State). The Secretary of State will only issue the warrant upon a determination that: (1) it is necessary for the protection of national security "for the purpose of preventing or detecting serious crime," or (2) it is necessary for the economic well-being of the United Kingdom. *See id.* IOCA requires the Secretary of State to ensure that less intrusive means of obtaining the information is not available prior to approving an interception. *See id.* Proposed electronic commerce legislation in the United Kingdom includes a provision that places the burden on the suspect to prove to law enforcement officers that they are not in possession of the requested keys. *See id* at 2.

240. *See supra* note 126 and accompanying text (providing the requirements for obtaining a court order to recover decryption keys and gain access to encrypted data).

241. *See id.*; *supra* note 239 and accompanying text (outlining the United Kingdom's procedures for issuing a warrant authorizing the interception of communications).

the United Kingdom, both Wassenaar members, have liberalized their encryption policies, recognizing that the overly burdensome regulation of encryption exports would hamper electronic commerce and the development of their respective technology industries.

In sum, the encryption debate forces nations to choose between promoting the growth of their technology sectors or providing law enforcement with enhanced tools to prevent crimes that are undetectable with current encryption technologies. As Germany and the United Kingdom demonstrate, the most developed economies are placing greater importance on the development of new technologies for export at the expense of security interests. Although security interests are important, the United States must heed the international community's warning and ensure that current Administration proposals, or independent legislative proposals, are enacted in a manner that permits domestic companies to regain their dominance in the global encryption market.

Fortunately, recent developments demonstrate that the Administration is willing to relax its current encryption export policy. The extent to which the United States will liberalize its encryption policy will remain unclear, however, until the Administration's September 1999 proposal is implemented. At the same time, the United States and the international community should monitor criminal activities and work with their respective private sectors to create alternative solutions to preserving the needs of law enforcement. More importantly, however, the international community must remain committed to establishing a binding and more inclusive international export control regime.