Journal of Legislation

Volume 26 | Issue 2 Article 6

5-1-2000

Re-Defining National Security in the Technology Age: The Encryption Export Debate;Note

Mark T. Pasko

Re-Defining National Security in the Technology Age: The Encryption Export Debate

I. Introduction

The technological revolution of the past decade has transformed the global economy. With the end of the Cold War, the United States and other industrialized nations have been able to re-direct significant portions of their economies away from defense spending and focus more of their attention on economic growth and development. The United States has encouraged its remarkable economic growth by reducing federal regulations and by encouraging free market principles. As a result, the American economy has greatly expanded in the 1990s, especially in the technology sector where America's leadership is unquestioned throughout the world.

Although the technological revolution has transformed the American economy, its national security policies have yet to reflect the progressive trends of this revolution. Traditional means of measuring a nation's strength, such as military power and natural resources, have given way to the importance of a nation's ability to collect, process, disseminate and protect information.[1] Establishing and maintaining America's technological dominance not only helps to deter or even prevent traditional military threats at a relatively low cost, but it also plays a significant role in fighting international terrorism, drug smuggling, and nuclear proliferation.[2] In order to protect its technological secrets and maintain its edge over other countries in acquiring and processing information, the United States has turned to encryption technology.[3] More specifically, encryption, the ability to transform and store text into an unintelligible form, now assumes a central role in continuing America's technological leadership and maintaining its national security.[4]

While encryption offers American industry a tremendous advantage in conducting its business by ensuring that transactions and industrial secrets are kept safe, encryption also offers many opportunities for misuse. Criminal activities that use encryption technology to their advantage, such as terrorism, organized crime, and industrial espionage have prompted the federal government to enact strong laws regulating encryption in order to prevent such misuse.[5] Many have argued that as a result of these regulations, America's lead in developing encryption technology has suffered by allowing foreign competitors to secure market share through the diminished presence of American industry in this area.[6] By weakening a vital part of the country's technology sector, American

---

1. Joseph S. Nye, Jr. and William A. Owens, *America's Information Edge*, 75 FOREIGN AFFAIRS, Mar. – Apr. 1996, at 20, 20.

2. *See id.*, at 20, 32.

3. Charles L. Evans, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C.J. INT'L L. & COM. REG. 469, 470 (1994).

4. Christian R. White, *Decrypting the Politics: Why the Clinton Administration's National Cryptography Policy Will Continue to be Dictated by National Economic Interest*, 7 CATH. U. COMM. L. CONSPECTUS 193, 194 (1999).

5. E. Franklin Haignere, *An Overview of the Issues Surrounding the Encryption Exportation Debate, Their Ramifications, and Potential Resolution*, 22 MD. J. INT'L L. & TRADE, Fall 1998 - Winter 1999, at 319, 319.

6. *See id.*, at 320.

regulations, in their effort to promote economic growth and strengthen national security, have actually damaged America's national security by hampering its technological growth. American policy treats encryption as a means to promote national security instead of an element of national security itself. This Note analyzes the legislative and legal treatment of encryption technology exports in an attempt to formulate a new understanding of national security as the United States moves into the twenty-first century. Furthermore, this Note acknowledges that although there have been significant attempts to ease restrictions on the export of encryption technology in recent years, there remains a strong need to create a national policy that balances both the security and economic interests of the United States.

II. Evolution of Encryption Technology

Although the methods of encryption have changed, encryption technology itself has existed for almost sixty years.[7] In World War II, encryption by means of mechanical devices, such as Germany's Enigma machines, was employed widely.[8] In the 1960s, mechanical encryption gave way to encryption performed by electronics and computers.[9] Because of its military potential, the United States government enjoyed a virtual monopoly on computer encryption until the 1970s, when IBM developed Lucifer, a commercial encryption device.[10] The primary purpose of Lucifer was cash-dispensing, although additional applications, both commercial and military, were envisioned.[11] After passing the government standards established by the National Bureau of Standards and the National Security Agency (NSA), IBM's Lucifer system was entrusted to protect all of the government's transmissions and storage of unclassified data and was certified as the new Date Encryption Standard (DES).[12] Today, the American economy primarily uses three encryption systems: DES, the original Lucifer system; RSA, named after its three inventors: Rivest, Shamir, and Adelman; and the Digital Signature Standard (DSS), developed jointly between the National Institute of Standards and Technology and the NSA.[13]

The utility of encryption rests on its ability to effectively protect the communication and information of its users. Without encryption, confidential information could be "intercepted or modified" by business competitors, or worse yet, by those willing to commit fraud, and used to the detriment of businesses and those seeking to do business with them.[14] Encryption prevents such adverse effects by applying a mathematical function, called an algorithm, to scramble data and other communications.[15] The algorithm used to unscramble, or decrypt, information is called the decryption key.[16] The strength of an encryption algorithm is measured by the "length of its key, which is measured in bits, and the complexity of its algorithm."[17] Each bit "doubles the number of possible key

7. Junger v. Daley, 8 F. Supp. 2d 708, 712 (N.D. Ohio 1988).

8. *See id.*

9. *See id.*

10. Mark B. Hartzler, National Security Export Controls on Data Encryption—How they Limit U.S. Competitiveness, 29 TEX INT'L L.J. 437, 440 (1994).

11. *See id.*

12. *See id.* at 440-41.

13. *See id.* at 441.

14. Mai-Tram B. Dinh, Note, *The U.S. Encryption Policy: Taking the Byte out of the Debate*, 7 MINN. J. GLOBAL TRADE 375, 379 (1998).

15. *See id.*

16. *See id.*

17. *Id.*

sequences; thus, as the number of bits increases, the encryption becomes dramatically stronger."[18]

Encryption technology is essential to the continued growth and success of electronic commerce (e-commerce) and the internet. The success of encryption in the global marketplace is evidenced by the subsequent growth of encryption products. In addition to the United States' encryption production, over 656 encryption products are manufactured by companies in approximately thirty countries throughout the world.[19] As a consequence of encryption's success and widespread use, the United States is faced with the challenge of balancing its need to compete economically by ensuring its encryption products are widely available in foreign markets while at the same time protecting its national security interests. The United States has enacted a series of regulations and oversight mechanisms to meet this challenge. These very regulations are at the center of the debate over whether or not strict controls on encryption exports actually increase national security.

III. Encryption Regulation

The current debate over encryption focuses on the export of that technology. Current regulations only affect exports and do not affect the "import, sale, [or] use of encryption products within the United States."[20] The export of encryption technology is controlled by the federal government under the Export Administration Regulations (EAR).[21] The EAR was established to implement the provisions of the Export Administration Act of 1979 (EAA), which was designed to "control exports of technology . . . which could make a significant contribution to the military potential of any country or combination of countries which would be detrimental to the national security of the United States."[22] The EAR defined "export" as "an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States."[23] In order to determine which items and activities fall under the EAR, one must consult the Commerce Control List (CCL).[24] As of March 1998, the CCL included over 200 sub-categories of controlled items and approximately 100,000 specific items.[25] Activities which fall under the EAR include encryption of commodities, software, and any technology with encryption features.[26]

In the past, the Department of State regulated encryption exports based on the authority of the Arms Export Control Act (AECA)[27] and the International Traffic in Arms Regulations (ITAR).[28] Central to the Department of State's review was the United States Munitions List (USML),[29] which classified encryption products as munitions,

18. *Id.* at 379-80, explaining that a "40-bit key allows more than a trillion possible combinations, while a 56-bit key allows more than 72 quadrillion possible combinations." *Id.* at 380. ("A skilled hacker can break the code for a 40-bit encryption key in about forty seconds . . . a 56-bit key require[s] 120 days to be broken, even with the power of a nationwide group of network computers. Today's fastest computers would require millions of years to descramble even stronger versions of encryption software.") *Id.* at 392.

19. F. Lynn McNulty, *Encryption's Importance to Economic and Infrastructure Security*, 9 DUKE J. COMP. & INT'L L. 427, 428-29 (1999). *See also*, Dinh, *supra* note 14.

20. Haignere, *supra* note 5, at 320.

21. Export Administration Regulations, 15 C.F.R. §§ 730-40 (1999).

22. 50 U.S.C. §2401 (1994).

23. 15 C.F.R. §734.2(b)(1) (1999).

24. 15 C.F.R. §734.2(a)(1) (1999).

25. White, *supra* note 4, at 197.

26. Haignere, *supra* note 5, at 321.

27. 22 U.S.C. § 2778 (1994).

28. 22 C.F.R. §§ 120-30 (1999).

29. United States Munitions List, 22 C.F.R. § 121.1, category XIII(b)(1) (1999).

thereby justifying government control over this technology.[30] Encryption software was included in the USML because of its capability to "maintain the secrecy or confidentiality of information or information systems."[31] Critics of the USML question its rigidity in failing to differentiate between encryption software used solely for military purposes and dual-use encryption software used by businesses and private citizens.[32] President Clinton's Executive Order 13,026, released on November 15, 1996, transferred the jurisdiction over dual-use software encryption software from the Department of State to both the Department of Commerce and the Department of State's Office of Defense Trade Control.[33]

The activities of the EAR are currently subject to the jurisdiction of the Bureau of Export Administration (BXA).[34] One of the BXA's primary functions is to regulate dual-use encryption software and place such software on the CCL.[35] After the Department of Commerce processes the application of the potential encryption exporter, the BXA then reviews it to determine whether or not export or re-export is consistent with U.S. national security interests.[36] Prior to September 1999, any individual or company seeking to export encryption technology over 56-bits in strength has to submit a license application to the Department of Commerce.[37] The Department of Commerce and the BXA thus play the central role of determining which U.S. encryption products are made available to foreign customers.

A. The United States Encryption Export Regime

Critics of strict regulations on encryption exports believe that these regulations go too far, serving neither economic nor national security interests. The first real public debate on encryption arose in 1993 over the Clinton Administration's key escrow-based Clipper chip proposal.[38] This proposal would have required every computer to contain an encryption key allowing the government access to any encrypted data.[39] The public outcry over seemingly endless government access to private information doomed this proposal, however.[40] Over the next few years, the Clinton Administration moved toward a more reasonable policy that emphasized the common interests of the government and the business sector on the issue of encryption.[41] By 1996, however, the software industry was restless for a modification of existing American law on encryption. Many encryption exporters argued in 1996 that "the pre-packaged software industry was estimated to be worth $109.3 billion and [was] expected to double to $221.9 billion by the year 2002."[42] Some analysts argued that current American encryption policies were costing U.S. companies an estimated $60 billion every year in lost revenue because international companies are allowed to export much stronger encryption technology than their American counterparts.[43] Until recently, U.S. companies could export 40-bit strength encryp-

30. Hartzler, *supra* note 10, at 444.
31. *Id.*
32. White, *supra* note 4, at 196.
33. *See id.*
34. *See* Haignere, *supra* note 5, at 320.
35. *See* 15 C.F.R. § 774, Supp. 1 (1999).
36. *See id.*
37. *See* Haignere, *supra* note 5, at 321. *See infra* text accompanying notes 90-92.
38. McNulty, *supra* note 19, at 431.
39. *See id* at 432.
40. *See id.* at 431-32.
41. *See id.* at 432.
42. White, *supra* note 4, at 201.
43. *See id. See also infra* notes 97-99 and accompanying text.

tion software with limited restrictions while their foreign competitors were allowed to export 128-bit strength encryption technology.[44] The loss of revenue and the growing unattractiveness of American encryption products threatened the loss of American competitiveness throughout the world.

The Clinton Administration has enacted a series of recent measures aimed at reforming the regulation of encryption exports. On May 8, 1997, the Clinton Administration changed its encryption policy relating to banks and financial institutions by allowing them to use the most powerful encryption technology without the use of a key recovery system.[45] In September 1998, Vice President Al Gore announced another shift in American encryption export policy on the issue of licensing requirements.[46] The policy called for the government, after a one-time review, to allow the mass marketing of 56-bit encryption technology, as opposed to the previously regulated 40-bit strength encryption products.[47] In addition, the Administration's new policy eliminated the requirement that companies create and implement a key recovery system. This means that companies that choose not to export key recovery technology no longer need to report information to a key recovery agent.[48]

With a growing number of countries producing and exporting sensitive encryption technology abroad, the Clinton Administration turned its attentions to creating an international regime on encryption controls. The NSA and the State Department in the past have consistently cited the dangers inherent in exporting encryption, including use by terrorists to facilitate attacks on American interests abroad.[49] Therefore, for any encryption export policy to be effective, the United States must gain the regulatory support of its allies and the major industrialized countries. The first attempt by the United States to rally international support to limit the export of sensitive technology like encryption came in 1949 with the formation of the Coordinating Committee for Multilateral Export Controls (COCOM), formed in conjunction with the North Atlantic Treaty Organization (NATO).[50] COCOM was designed to coordinate the export policies of its members and provide oversight for exports to suspect nations in an effort to form a more cohesive export regime.[51]

In an effort to refocus its allies' interests on the importance of limiting the export of encryption technology to rogue states, the Clinton Administration sought to establish a new COCOM for the next century in the form of the Wassenaar Agreement in December 1998.[52] The Wassenaar Agreement was formed by thirty-three industrialized nations with the specific goal of restricting exports of military and military-civilian "dual-use" technology to renegade countries such as Libya, Iran, and North Korea.[53] The Wassenaar group's Dual-Use Control List extended to encryption products using over 56-bits, including "web browsers, e-mail applications, e-commerce servers, and telephone scrambling devices."[54] In addition, the Wassenaar countries agreed to improve their

---

44. *See id. See also infra* notes 126-27 and accompanying text.

45. White, *supra* note 4, at 200.

46. McNulty, *supra* note 19, at 433.

47. White, *supra* note 4, at 200.

48. *See id.* at 200-01.

49. *See id.* at 198.

50. Hartzler, *supra* note 10, at 442 (COCOM's current members include Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Spain, Turkey, the United Kingdom, and the United States).

51. *See id.*

52. McNulty, *supra* note 19, at 435.

53. *Id.*

54. *Id.*

national controls on the export of encryption products with strengths over 64-bits, which applied to items such as personal computers and data base programs.[55]

Although the Wassenaar Agreement did ensure the free flow of encryption products under 56-bit, many critics, in the United States and abroad, point out that restricting the export of encryption products violates free speech rights. More specifically, they claim that the Wassenaar restrictions violate international protections against arbitrary interference with individual privacy and the free expression of ideas. Anticipating Wassenaar's new restrictions, in September 1998, Human Rights Watch criticized the proposed agreement by warning that coded language communications are protected as a right of free expression under the International Covenant on Civil and Political Rights, to which most members of the Wassenaar are parties.[56] The efforts of Human Rights Watch highlight the complexity of the encryption export debate both in the United States and abroad.

B. American Courts on Encryption

American courts are sharply divided over whether or not regulating the export of encryption products is a violation of the law. Three cases in particular, *Karn v. United States Department of State*,[57] *Bernstein v. United States Department of State*,[58] and *Junger v. Daley*[59] all highlight the current confusion in the courts and the industry over what constitutes a violation of America's encryption export policy. The failure of these courts to reach a consensus reflects the complexity of the issue and the embryonic state of American law on the regulation of encryption exports.

1. Karn v. United States Department of State

The dispute in *Karn* arose when the State Department classified the plaintiff's computer diskette "as a 'defense article' pursuant to the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR)."[60] In February 1994, plaintiff, Philip R. Karn, Jr., submitted a commodity jurisdiction request to the State Department for Bruce Schneier's book, *Applied Cryptography*, which contained information on encryption protocols, techniques, and algorithms.[61] On March 2, 1994, the State Department's Office of Defense Trade Controls (ODTC) "determined that the book [was] not subject to the jurisdiction of the Department of State pursuant to the ITAR,"[62] although this determination did not extend to two diskettes containing an encryption source code discussed in *Applied Cryptography*.[63] Mr. Karn submitted an additional commodity jurisdiction request just one week later for the diskette; the request was soon rejected on the basis that the diskette was "subject to the jurisdiction of the Department of State pursuant to the ITAR and the AECA because the diskette 'is designated as a defense article under category XIII(b)(1) of the United States Munitions List.'"[64]

---

55. *See id.* The Wassenaar Agreement is discussed at length *infra* p. 26
56. *See id.* at 436.
57. 925 F. Supp. 1 (D.D.C. 1996).
58. 974 F. Supp. 1288 (N.D. Cal. 1997).
59. 8 F. Supp. 2d 708 (N.D. Ohio 1998).
60. *See Karn*, 925 F. Supp. at 2.
61. *See id.* at 3.
62. *Id.*
63. *See id.*
64. *Id.* at 4.

The primary contention by the plaintiff in *Karn* was that the State Department's regulation of the diskettes constituted "a restraint on free speech in violation of [his] First Amendment rights."[65] More specifically the plaintiff argued that:

> the diskette should be considered 'speech' for the purpose of First Amendment analysis because the computer language source codes contained on the diskette are comprehensible to human beings when viewed on a personal computer, because the diskette contains 'comments' interspersed throughout the source code which are useful only to a human and are ignored by the computer, and because the source ode and comments taken together teach humans how to speak in code.[66]

In rejecting Karn's First Amendment complaint, the court based its decision on the need of the federal government to regulate items which have national security implications. The court held that the regulation of Karn's diskettes was content-neutral and capable of regulation by the government as long as other criteria were met, as opposed to content-specific, which would bar government regulation of such materials.[67] The additional criteria include "whether the regulation is (1) within the constitutional power of the government, (2) 'furthers an important or substantial government interest,' and (3) is narrowly tailored to the government interest."[68] The court reasoned that the government regulation of Karn's diskettes passed the O'Brien Test because by "placing cryptographic products on the ITAR, the President has determined that the proliferation of cryptographic products will harm the United States."[69] Furthermore, the court was reluctant to question the President's foreign policy decision on encryption or to define American national security interests, which are the exclusive province of the executive and legislative branches of government.[70]

2. Junger v. Daley

Junger v. Daley further supported government regulation of encryption exports. In this case, the plaintiff, Peter Junger, was a law professor at Case Western Reserve University Law School in Ohio and taught a class entitled "Computers and the Law."[71] On June 12, 1997, Professor Junger submitted three applications to the Department of Commerce in order to receive a commodity classification for several encryption software programs and other items he needed as part of his class materials.[72] Professor Junger was notified by the Bureau of Export Administration on July 4, 1997 "that Export Classification Number 5D002 covered four of the five software programs he had submitted, and therefore were subject to the Export Regulations."[73] Despite the limitations imposed on the export of his software programs, Professor Junger was allowed to export the chapter in his textbook, *Computers and the Law*, which pertained to encryption.[74] The Department of Commerce decided that the chapter of his book on encryption

---

65. *Id.* at 9.

66. *Karn*, 925 F. Supp. at 9.

67. *See id.* at 10.

68. *Id.* This test is also known as the "O'Brien Test" established in *United States v. O'Brien*, 391 U.S. 367 (1968).

69. *Id.* at 11.

70. *See id.* at 11-12.

71. *Junger*, 8 F. Supp. 2d at 713.

72. *See id.* at 714.

73. *Id.*

74. *See id.*

code was free for export but that if he wanted to export his software programs, Professor Junger would first have to seek a license for those items.[75]

Professor Junger filed suit in October, 1997 against William Daley, the Secretary for the Department of Commerce, claiming the Export Regulations violated his First Amendment right to free speech. In deciding whether or not the Export Regulations constituted a violation of Junger's free speech, the court had to determine whether the export of encryption code was "expressive, and whether the Export Regulation [was] directed at the content of ideas."[76] The U.S. District Court, in ruling that the content of Professor Junger's encryption software was not expressive, held that:

> Among computer software programs, encryption software is especially functional rather than expressive. Like much computer software, encryption source code is inherently functional; it is designed to enable a computer to do a designed task. Encryption source code does not merely explain a cryptographic theory or describe how the software functions. More than describing encryption, the software carries out the function of encryption. The software is essential to carry out the function of encryption. In doing this function, the encryption software is indistinguishable from dedicated computer hardware that does encryption. In the overwhelming majority of circumstances, encryption source code is exported to transfer functions, not to communicate ideas.[77]

The court went on to reason that although exporting source code "occasionally" [78] has communicative elements, that remains insufficient to extend the protections of the First Amendment to it. The court's reasoning suggests that had the encryption software been found to communicate ideas, application of the Export Regulations would be unconstitutional under the First Amendment. *Junger*, therefore, supported the Export Regulations of encryption software because source code is inherently functional, such regulations are not directed at the expressive elements of source code, and Professor Junger still was able to export the printed form of this information.[79]

3. Bernstein v. United States Department of State

Despite the rulings in *Karn* and *Junger*, the American judiciary remains divided on the constitutionality of regulating encryption technology and its implications on the First Amendment guarantee to free speech. *Bernstein v. United States Department of State*, which was decided after *Karn* but before *Junger*, took the other side of the issue and favored First Amendment protection of encryption technology exports. *Bernstein* serves as a reminder not only of the courts' split on the issue of First Amendment protection for encryption exports, but also on the need for legislative reform on this issue.

While a graduate student at the University of California at Berkeley, Daniel Bernstein developed an encryption algorithm called "Snuffle."[80] Mr. Bernstein expressed this algorithm in an academic paper entitled "The Snuffle Encryption System" and in source code written in "C," a type of computer programming language.[81] In 1992, Mr. Bernstein submitted a commodity jurisdiction request to the State Department to determine whether his Snuffle program and related encryption items were subject to the ITAR.[82]

---

75. *See id.*
76. *Id.* at 715.
77. *Junger*, 8 F. Supp. 2d at 716.
78. *Id.* at 717.
79. Haignere, *supra* note 5, at 330.
80. *Bernstein*, 974 F. Supp. at 1293.
81. *Id.*
82. *See id.*

The Office of Defense Trade Controls (ODTC) determined that the Snuffle program was a defense article on the USML under Category XIII of the ITAR and subject to export licensing regulations.[83]

Mr. Bernstein filed his action based on the ODTC's determination that his Snuffle program was a defense article under the USML. Specifically, Mr. Bernstein believed that the regulations of the ITAR and the AECA violated his First Amendment rights by limiting his freedom to teach, publish, or discuss with other scientists his research on encryption.[84] Also, Mr. Bernstein contended that the EAR and the regulations on encryption items, not only restrained his free speech, but were unconstitutionally vague and over-broad, content-based, and a violation of his freedom of association.[85] The court in *Bernstein* acknowledged that governments may impose certain restrictions on materials that are "content neutral, narrowly tailored to serve a substantial governmental interest, and leave open alternative channels for communication."[86] Because the court had already determined in previous decisions that source code constituted expressive activity, it turned its attention to the licensing procedure used by the Department of Commerce.[87] The court relied on *Freedman v. Maryland*,[88] which held that in order for a licensing regime to be constitutional, "1) the licensor must make the licensing decision within a specific and reasonable period of time; 2) there must be prompt judicial review; and 3) the censor must bear the burden of going to court to uphold a licensing denial and once there bears the burden of justifying the denial."[89] In finding that the export restrictions on Mr. Bernstein's encryption software were unconstitutional, the court reasoned:

> This court has stated previously that while it is mindful of the problems inherentin judicial review of licensing decisions regarding cryptographic software, both withrespect to the sophistication of the technology and the potentially classified natureof the licensing considerations, there must still be some review available if the exportcontrols on cryptographic software are to survive the presumption against prior restraintson speech. In this case . . . the court concludes that the encryption regulations are an unconstitutional prior restraint in violation of the First Amendment.[90]

The *Bernstein* decision, when considered with *Karn* and *Junger*, highlight the need for the government to balance the interests of free speech and national security. They also demonstrate that current federal regulations must be revised in order to effectively address these issues and formulate a stronger encryption export policy.

IV. Creating a Stronger Encryption Export Policy

In order to create a more effective encryption export regime, American encryption policy should acknowledge the interrelationship between economic and national security interests. Limiting the enforcement of encryption regulations to the United States will do little to deter terrorists or criminals from using encryption as long as those individuals can obtain such material from other industrialized nations. Furthermore, allowing a rigid encryption export regime punishes American companies because as these companies

---

83. *See id.*

84. *See id.*

85. *See id.* at 1296.

86. *Bernstein*, 974 F. Supp. at 1303.

87. Haignere, *supra* note 5, at 334 (citing *Bernstein v. United States Department of State*, 922 F.Supp. 1426 (N.D. Cal. 1996)(Bernstein I) and *Bernstein v. United States Department of State*, 945 F.Supp. 1279 (N.D. Cal. 1996)(Bernstein II).

88. 380 U.S. 51 (1965).

89. *Bernstein*, 974 F.Supp. at 1308 (citing *Freedman*, 380 U.S. at 58-60).

90. *Id.*

comply with tight regulations, their foreign competitors gain market share at their expense. Such a result not only denies American companies potential profits but also threatens the competitiveness of the encryption industry. This challenge calls for leadership by the United States government in working with other countries to meet the shared threats of international crime and terrorism. Enhanced international cooperation along with domestic regulatory reform will strengthen the United States' encryption industry and in doing so, further American security interests.

A. Domestic Encryption Regulation Reform

The first step in creating an effective and lasting encryption export regime starts with the creation of adequate domestic regulations. U.S. laws addressing encryption so far have created confusion and have drawn fire from various groups for either favoring economic interests too much or not doing enough to safeguard national security interests. One piece of legislation currently before Congress is the Security and Freedom Through Encryption (SAFE) Act of 1999,[91] which makes significant progress in addressing the concerns of the various parties to the encryption debate.[92] The SAFE Act represents an attempt to weigh the desires of the encryption industry to liberalize the export of its products with the interests of national security in fighting international terrorism, espionage and domestic criminal acts. Although by no means a panacea, the framework of the SAFE Act addresses the encryption concerns of today while making future reform possible as the encryption industry grows and new challenges to America's national security emerge.

1. Law Enforcement

In a move to appease the encryption industry, President Clinton announced a new policy on September 16, 1999 that would "dramatically ease restrictions on overseas sales of sophisticated encryption products [and] the technology that scrambles electronic data so it cannot be read without authorization . . ."[93] This statement drew criticism from law enforcement officials within the government and throughout the country. Attorney General Janet Reno warned that "the policy the administration is announcing today will result in greater availability of encryption, which will mean that more criminals and terrorists will use encryption."[94] The opinions expressed by Attorney General Reno and others showed a genuine fear that without adequate controls on the export of encryption technology, the ability of law enforcement officials to capture and prosecute criminals and terrorists will be greatly reduced.[95]

---

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

92. *See* Haignere, *supra* note 5, at 346. The original SAFE Act, known as H.R. 695, was introduced in 1997 but stalled in committee. *See id.* H.R. 695 would have eliminated all restrictions on the use of encryption software by citizens in the United States, placed oversight of encryption exports with the Department of Commerce, allowed for the export of encryption products that were widely available overseas and the use of encryption software to further a criminal act illegal. *See id.*

93. Jonathan Rabinovitz, *U.S. Encryption Limits to be Eased*, SILICON VALLEY NEWS, ¶2 (Sept. 15, 1999) <http://www.mercurycenter.com/svtech/news/indepth/docs/enc091699.htm..> President Clinton's policy consisted of three pillars: providing the Department of Defense $500 million over several years to improve its information security, easing the export license restrictions on keys of 128 bits or more, and the introduction of legislation aimed at improving America's law enforcement methods in dealing with encrypted messages. *See id.* at ¶¶ 10-12..

94. David Wilson, *Encryption in Crossfire*, SILICON VALLEY NEWS, ¶3 (Sept. 16, 1999) <http://www.mercurycenter.com/svtech/news/indepth/docs/enc091799.htm.>

95. *See* White, *supra* note 4, at 198 (referring to the Aldrich Aimes and Ramzi Yousef cases as examples of criminals who have used encryption technology to hide their criminal activity and avoid prosecution).

The SAFE Act addresses many of the concerns presented by Attorney General Reno and others in law enforcement. In an effort to clarify the penalties for those using encryption technology in furtherance of their criminal behavior, the Act amends title 18, §2805 of the United States Code to include:

> Any person who, in the commission of a felony under a criminal statute of the United States, knowingly and willfully encrypts incriminating communications or information relating to that felony with the intent to conceal such communications or information for the purpose of avoiding detection by law enforcement agencies or prosecution (1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined in the amount set forth in this title, or both; and (2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined in the amount set forth in this title, or both.[96]

The Act also provides the Attorney General and law enforcement officials with additional powers with which to monitor criminal activities. The Act provides that "[t]he Attorney General shall compile, and maintain in classified form, data on the instances in which encryption has interfered with, impeded, or obstructed the ability of the Department of Justice to enforce the criminal laws of the United States."[97] Strengthening the hand of law enforcement has become even more important in the wake of recent attacks on internet business. The recent success of hackers in disabling the websites of Yahoo!, Buy.com, eBay, Amazon.com and CNN.com highlights the need not only for tougher sentencing for criminals who use encryption to commit and hide their illegal activity, but also for more sophisticated measures to prevent these crimes from occurring in the first place.

2. Protecting the Encryption Industry

On the opposite side of the debate is the encryption industry, which maintains that restrictions on the export of encryption technology do more harm to vital national interests than terrorists or criminals ever could. Many of America's software companies believe that the "demand for information security is increasing so rapidly and becoming so widespread that American companies stand to lose billions in annual revenue and tens of thousands of jobs" if strict encryption export controls remain in place.[98] These fears were substantiated by a 1998 report issued by the Economic Strategies Institute (ESI) which stated that the U.S. economy stood to lose upwards of $97 billion over the next five years as a result of current encryption export regulations.[99] ESI's report estimated that American companies could lose an additional $140 billion in overseas sales because foreign buyers would shy away from American software and other products that were not protected by adequate encryption measures.[100] The current encryption export regime thus leaves the industry in the United States with two options: (1) lose market share to foreign competitors or (2) develop two versions of their encryption software, one of domestic use and one for export. The pitfalls of the second option are clear when one considers that encryption developers would essentially have to develop two different products, leading to a tremendous drain on their financial resources.[101] Companies

96. H.R. 850, 106th Cong. § 2 (1999) (amending 18 U.S.C. § 2805).

97. H.R. 850, 106th Cong. § 4 (1999).

98. Evans, *supra* note 3, at 489 (citing Bob Violino, *Gore Rebuffs Software Industry*, INFORMATIONWEEK, Feb. 7, 1994, at 15).

99. *See* McNulty, *supra* note 19, at 444.

100. *See id.*

101. *See* Evans, *supra* note 3, at 489-90.

which could not afford to develop two versions of their encryption software would have to either limit themselves to domestic sales and deny themselves foreign market share or export the "weaker" version and be noncompetitive in foreign markets.[102]

The recent initiatives of President Clinton and the provisions of the SAFE Act take steps towards protecting the American encryption industry. President Clinton's September 1999 address signaling an easing of export limitations on encryption products should provide a financial boost to leading encryption companies and promote more uniformity throughout the entire e-commerce industry.[103] The SAFE Act has also brought its own set of benefits to the encryption industry when it amended the Export Administration Act of 1979[104] by overhauling its licensing regime and introducing clearer standards of when companies can and cannot export encryption technology. According to the SAFE Act, no export license is required:

> [a]fter a one-time technical review by the Secretary of not more than 30 working days, which shall include consultation with the Secretary of Defense, the Secretary of State, the Attorney General, and the Director of Central Intelligence . . . except pursuant to the Trading with the Enemy Act or the International Emergency Powers Act.[105]

This provision applies to:

> Any computer hardware or software or computing device, including computer hardware or software or computing devices with encryption capabilities that is generally available; that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or that is used in a commercial, off-the-shelf, consumer product or any component or subassembly designed for use in such a consumer product available within the United States or abroad which includes encryption capabilities which are inaccessible to the end user; and is not designed for military or intelligence end use.[106]

The SAFE Act also clarifies the rules on when exporting is not permitted. These restrictions will apply when there is:

> substantial evidence that such computer hardware or software or computing devices will be diverted to a military end use or an end use supporting international terrorism; modified for military or terrorist end use; reexported without any authorization by the United States that may be required under this Act; or (1) harmful to the national security of the United States, including capabilities of the United States in fighting drug trafficking, terrorism, or espionage, (2) used in illegal activities involving the sexual exploitation of, abuse of, or sexually explicit conduct with minors, or (3) used in illegal activities involving organized crime.[107]

Such provisions should provide some guidance to potential encryption exporters and eliminate some confusion in this area of the law.

Another move that would ease restrictions on the export of certain encryption software would be to reform the United States Munitions List and streamline departmental oversight of encryption exports. One of the main failings of the USML is its failure to

---

102. *See id.*
103. *See* Rabinovitz, *supra* note 93, at ¶4.
104. 50 U.S.C. §2416 (1979).
105. H.R. 850, 106th Cong. § 7 (1999).
106. *Id.*
107. *Id.*

adequately resolve the problem of dual-use technologies.[108] Current regulations authorize the President to "control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services."[109] The chief complaint of the encryption industry in the United States is the categorization of their products as either defense articles or defense services.[110] The inclusion of "cryptographic systems"[111] alongside items such as bombs,[112] grenades,[113] tanks,[114] and ballistic missiles[115] suggests the need to rethink what kind of national security threat encryption software presents.[116]

Passage of the SAFE Act and reform of the USML would address many of the concerns of the encryption industry in the United States by simplifying the licensing process for encryption software, establishing clear export criteria for companies and making special provisions for dual-use encryption technology. The question of when to export encryption technology, however, cannot be resolved by presidential policy speeches and House bills. There is a very real and pressing need in the wake of recent internet "piracy" and the growing role of high technology in our everyday lives to redefine national security as the United States moves into the twenty-first century. A country's position in the international arena is no longer measured by how much military power it can bring to a field of battle or how many strategic assets it possesses.[117] Today, America's strength is judged by numerous economic factors including industrial production, economic growth, unemployment, and the success of the stock market.

3. Defining the "New" National Security Policy

The dynamics of a global economy call for new leadership on the question of encryption technology which recognizes that protecting the competitiveness of American business is just as important as the ability to deploy military forces abroad. Internet piracy and the damage it does to corporate networks and e-commerce is a relatively new byproduct of the technology age and should serve as a wake-up call to the politicians of America to recognize that the well-being of America's business interests is the emerging national security priority of the twenty-first century. Furthermore, current encryption export restrictions pose a danger to the security of the internet. The Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG), two of the international groups responsible for "technical management and standards development" for the internet, have warned that current American encryption policy makes the internet vulnerable to criminal assaults on electronic commerce.[118] The IAB and the IESG also

108. *See* White, *supra* note 4, at 196.

109. 22 U.S.C. § 2778(a)(1) (1999).

110. *See* Evans, *supra* note 3, at 477-78.

111. 22 C.F.R. §121.1 Category XIII(b)(1) (1993).

112. *See id.* §121.1 Category IV(a).

113. *See id.*

114. *See id.* §121.1 Category VII(a).

115. *See id.* §121.1 Category IV(b).

116. Evans, *supra* note 3, at 477. 22 C.F.R. §121.1 Category XIII(b)-(b)(1) includes "military information security systems and equipment, cryptographic devices, software, and components specifically designed or modified therefor (i.e., such items when specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications)). This includes: (1) military cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, including equipment and software for tracking, telemetry and control (TT&C) encryption and decryption."

117. *See* Nye and Owens, *supra* note 1, at 20.

118. McNulty, *supra* note 19, at 448.

said that American encryption export restrictions will hurt developing countries that lack the financial and technical resources to develop their own encryption software.[119] The proposed $2 billion for Fiscal Year 2001 for cyber-security by the Clinton Administration is a start but is still woefully inadequate to the task of protecting America's economic interests.[120]

Encryption plays a central role in strengthening America's economic interests against cyber threats. Improving America's laws and providing additional funding, however, will prove fruitless in addressing these threats if the United States is unable to obtain cooperation from countries around the world. Although the United States has more to lose from internet piracy now due primarily to the widespread use of the internet throughout American society, threats to e-commerce will eventually impact the entire international community and threaten the growth of the world economy. Any encryption strategy, therefore, must take into consideration the importance of international cooperation in any solution to information security.

B. International Encryption Oversight and Cooperation

The encryption export policies of the United States during the Cold War reflected its economic, political and military preeminence. In an effort to create a liberal international economic regime which protected its national security interests, the United States passed the Export Control Act of 1949 (ECA).[121] The ECA provided the President with the powers to "prohibit the commercial export of articles, materials, or supplies, including technical data, to nations unfriendly to the United States."[122] As long as the Soviet military threat lingered, America's allies in Europe and Asia were willing to follow its lead. Since the end of the Cold War, however, America's traditional allies have little to gain by following America's notions of national security. These allies now see organizations such as COCOM and other international regimes driven by the United States as tools of furthering American dominance in an emerging technology sector. Today, the challenge to America's leaders is to convince industrialized nations that there are threats to global security, not just American national security. America's efforts to enforce strict encryption export controls will have limited success without the cooperation of the international community.

Over the past decade, the United States has had mixed success in building a consensus among the international community on the issue of encryption export regulations. One of the most serious blows to American encryption policy came on October 8, 1997 from the European Commission (EC), which regulates the trade of the fifteen members of the European Union (EU).[123] The EC announced that it would not join an American ban on certain encryption exports, citing the potential that such an action would stifle the growth of e-commerce and would be difficult to enforce.[124] The EC's refusal to follow America's lead on encryption export regulations is evidence of the changing atmosphere following the Cold War. Today, countries do not see America's global economic and political power as a reason to follow the American lead, but rather, they view it as a challenge to compete more robustly in the international marketplace.

---

119. *See id.*

120. *See Clinton to Meet Internet Leaders on Cyber Threats*, REUTERS, (Feb. 11, 2000), <http://www.mercurycenter.com/svtech/news/breaking/merc/docs/007585.htm.>

121. *See* Hartzler, *supra* note 10, at 441.

122. *Id.*

123. *See* Dinh, *supra* note 14, at 389.

124. *See id.* at 389-90. The EC reasoned that joining a strict encryption export regime would hurt the development of this emerging market. *See id.*

Some progress was achieved in the area of encryption export regulation with the Wassenaar Agreement in December 1998.[125] Wassenaar was able to bring thirty three industrial nations together and agree to bans on the export of dual-use technologies to rogue states which included the export of 56-bit encryption keys.[126] The momentum gained by Wassenaar was lost the following month, however, when one of its member countries, France, announced it was dropping all controls on encryption technology up to 128-bits.[127] In raising its export threshold from 40-bits to 128-bits, the French government cited its desire to improve the ability of its citizens to protect their confidential communications and its wish to remove obstacles to the growth of e-commerce.[128] The French government's announcement highlights resistance to American encryption export regulations not just in France, but throughout the international community, forcing the United States to rethink its encryption priorities and develop a new strategy.

President Clinton's September 1999 policy initiative easing export license restrictions on encryption keys with at least 128-bit strength suggests a policy in which the United States joins other countries in exporting stronger encryption products in an attempt to influence the export policies of those countries. In many ways, the United States encryption software industry is a victim of its own success. Countries perceive America's initiatives on regulating encryption exports as a means of perpetuating American dominance in this industry. It is easy to understand that in the absence of any real security threat, America's allies would risk this technology falling into the hands of terrorists or criminals if it meant a chance for them to cut into America's dominance in the encryption market. Despite the vociferous complaints of the American encryption industry over U.S. policy, recent information suggests that the encryption industry has not lost any real market share to foreign competitors in the 1990s despite relatively strong export controls.[129] Furthermore, the Clinton Administration has not perceived a threat from foreign competition in the encryption industry mainly because "[t]he mere fact that other countries produce encryption programs of some strength does not prove that they can capably compete with U.S. manufacturers with respect to the strong technologies addressed in the Administration's regulations."[130]

With this in mind, the reasons behind President Clinton's September 1999 encryption policy announcement become less clear. If the Administration is not concerned with foreign competition, what, then, is the policy objective behind the September 1999 policy statement? There are several likely reasons behind the Administration's recent policy shift. First, if the United States has a majority of the market share for encryption products, liberalizing U.S. licensing regulations would help American industry maintain their industry-wide lead that much more. Second, President Clinton's policy speech recognizes the fact that the technology in this field is progressing much faster than the law regulating it. American corporations are already protecting their business information with software exceeding 128-bits, and more businesses in the United States and throughout the world can be expected to move past this level of data protection. Third, by easing the restrictions on the export of encryption technology, the United States has placed itself in a better position to work with other countries in establishing an effective encryption export regime.

---

125. *See supra* notes 52-56 and accompanying text.

126. *See* McNulty, *supra* notes 51-54.

127. *See id.* at 441.

128. *See id.*

129. *See* Dinh, *supra* note 14, at 391 (citing Greg Rattray, *The Emerging Global Information Infrastructure and National Security*, 21 FLETCHER F. WORLD AFF. 81, 88 (1997)(explaining that of the more than 1000 encryption products manufactured throughout the world, only 435 were not produced in the United States).

130. Dinh, *supra* note 14, at 391-92.

The problem with creating an effective system of regulating encryption exports throughout the world is that countries have been unwilling to coordinate their national policies in this area. One of the primary reasons for this is the fact that approximately thirty nations manufacture encryption products and most of the encryption industries in these countries are just in their infancy, making plans of global regulation a very difficult sell. As the encryption industries in these countries mature and the use of encryption software becomes more widespread, America's concerns over criminal use of encryption and internet terrorism will eventually be acknowledged and shared throughout the world.

Instead of trying to promote encryption regulation unilaterally, the United States should work within existing international regimes such as Wassenaar or the World Trade Organization (WTO). Both Wassenaar and the WTO have institutional machinery already in place to provide the framework for creating a more lasting encryption export regime. A multilateral approach to the encryption export debate would have the effect of coordinating international policy by expanding the scope of encryption regulation while reducing the incentive of individual nations to pursue their own encryption policies. A unilateral approach by individual nations would be detrimental to the international community and global information security.

V. Conclusion

The United States is at a crossroads in defining its national security interests as it moves into the twenty-first century. The absence of a clear geopolitical rival, however, does not mean that the United States is without challenges to its national interests. Indeed, the past decade has given rise to a global economy in which countries once bound together in common defense during the Cold War now find themselves competing with one another for global market share. Today, protecting American industry and economic growth has become as important as maintaining its military strength.

America's encryption export policy is caught in the middle of this transformation of America's national security priorities. Since World War II, the United States has favored tight controls on the export of encryption technology in an effort to limit the access of Soviet-bloc nations to this resource. With the Cold War over, America's controls on encryption exports still remain in the form of strict licensing requirements and simplistic categorization of encryption products as defense articles.[131] The main reason for this is the failure to understand encryption, not as a threat, but as a vital part of America's national security as it moves into the next century. Encryption products are vital to the security of information passed on the internet and business networks and play an important role in the expansion of the global economy. Protecting American industry has emerged as the new American national security interest in a competitive global market place. Encouraging the encryption industry by revising America's export policies of this technology is an integral part of protecting this aspect of our national security.

The solution to the encryption export debate is based on legislative action and international cooperation. The desire to encourage the encryption industry and its role in protecting American commerce across the globe should be considered in conjunction with the concern of its misuse in furtherance of terrorist or criminal acts. The SAFE Act of 1999 and policy initiatives by the Clinton Administration have balanced industry attempts to liberalize the current encryption export regime with measures which strengthen the power of local and federal law enforcement agencies to combat criminals.

131. *See supra* notes 97-99, 107-15 and accompanying text.

In addition to reforming domestic encryption regulations, the United States needs to foster closer international cooperation concerning encryption exports. The trend in recent years is for countries to unilaterally pursue their own interests and export encryption products without regard to the security implications of their decisions.[132] Convincing the encryption-producing nations of the world of the need for a coordinated policy which balances legitimate national economic interests with international security is arguably the toughest challenge facing the United States today on this issue. The implementation of recent policy initiatives and legislation, however, would strengthen the position of the United States in encouraging other nations to work within existing regimes and in fostering their cooperation in creating a lasting encryption export regime.

*Mark T. Pasko**

132. *See supra* notes 126-27 and accompanying text.

* B.A., Government and History, Georgetown University, 1995; M.S., International Relations, London School of Economics and Political Science, 1996; Juris Doctor Candidate, Notre Dame Law School, 2001.