THE ENCRYPTION EXPORT TAX: A PROPOSED SOLUTION AND REMEDY TO THE ISSUES AND COSTS ASSOCIATED WITH EXPORTING ENCRYPTION TECHNOLOGY

*John L. Paik**

* B.S., Cornell University, 1994; M.S., University of California, Los Angeles, 1997; candidate for J.D., Cornell Law School, 2001. I dedicate this Note to my parents and my sister, Gina.

INTRODUCTION

U.S. regulations on the export of encryption technology ("crypto") raise numerous complex issues with technical, political, legal, and economic dimensions. The main argument for regulating and restricting the export of encryption is that the abuse of this technology by terrorists and criminals would severely impede the ability of national security and law enforcement officials to carry out their functions.[1] The software and high-tech industries, on the other hand, argue that current export regulations put U.S. encryption businesses at a competitive disadvantage relative to foreign companies, and that such regulations violate their First Amendment free speech rights.[2] Privacy advocates, who are on the same side of the debate as the high-tech industries, argue that any restrictions on the accessibility of encryption products infringe on the individual's right to informational privacy, thus implicating the Fourth Amendment.[3]

The government does not deny the importance of strong encryption to U.S. companies and private citizens alike.[4] Encryption products

> both serve to protect proprietary data of U.S. companies worldwide and have the potential to be an economic boom in the cryptography software market . . . . [T]he problem is reconciling all of these competing interests and sorting out the extremes, which are numerous, but without compromising any one interest too much.[5]

In order for the U.S. government to reach this middle ground, it must strike a balance between America's national security interests on one hand, and commercial and privacy interests on the other: "The government must meet the responsibility of enhancing public safety and national security, but the requirements that it imposes should not be so

---

[1] *See* FBI, ENCRYPTION: IMPACT ON LAW ENFORCEMENT (June 3, 1999) at 1 [hereinafter FBI REPORT] (stating that "[t]he law enforcement community . . . is extremely concerned about the serious threat posed by the proliferation and use of robust encryption products that do not allow for the immediate, lawful access to the plaintext of encrypted, criminally related communications . . . .").

[2] *See* Jeri Clausing, *Concerns Raised Over Encryption Report*, N.Y. TIMES, Nov. 24, 1999, at C5.

[3] *See generally Americans for Computer Privacy* [hereinafter ACP] *at* http://www.computerprivacy.org (last visited Feb. 23, 2000).

[4] *See* FBI REPORT, *supra* note 1.

[5] J. Terrence Stender, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 CASE W. RES. J. INT'L L. 287, 321 (1998).

burdensome as to hinder the development of products that incorporate encryption technology."[6] To this end, this note proposes that the U.S. government continue with its current trend of easing export restrictions on encryption technology, and in place of licensing restrictions introduce a less burdensome "encryption export tax." The revenue from this tax would then be used to fund a joint and centralized effort by the Federal Bureau of Investigation ("FBI")[7] and the National Security Agency ("NSA")[8] to research and develop advanced decryption technologies and tools.

The first section of this note introduces the basics of encryption and defines the commonly used terms within the field of cryptography. The next section outlines the current regulations and agreements, both at the domestic and international levels, as well as pending proposals to amend U.S. regulation of encryption exports. This note then provides a historical overview of the development of encryption technology, as well as the governmental policies and regulations regarding this technology. Next, this note will delve into the constitutional issues at the heart of governmental regulation of encryption technology. This note then analyzes the arguments for protecting national security interests through the regulation of encryption exports, as well as the arguments for liberalizing such regulations. Finally, this note proposes implementing an "encryption export tax" to fund governmental counter-encryption research and development in lieu of regulating of encryption exports.

I. ENCRYPTION BASICS AND TERMINOLOGY

Cryptography is the art of using code to keep information secret.[9] *Encryption* is a technique or process for encoding or scrambling communications so that information exchanged between two or more parties is kept confidential and does not, in the course of communication, become known to anyone other than the sender and the receiver.[10] The unencrypted information is referred to as *plaintext*, whereas the encrypted version of this same information is known as *ciphertext*.[11] *Decryption* is

---

6 Christian White, *Decrypting the Politics: Why the Clinton Administration's National Cryptography Policy Will Continue to be Dictated by National Economic Interest*, 7 COMMLAW CONSPECTUS 193, 202 (1999).

7 The FBI, established in 1908, is responsible for "investigating all violations of federal laws with the exception of those which have been assigned by legislative enactment or otherwise to some other Federal agency." BLACK'S LAW DICTIONARY 625 (7th ed. 1999).

8 The NSA, established in 1952, is a division of the Department of Defense. STEWARD A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST: CRYPOGRAPHY, GOVERNMENTS, AND ELECTRONIC COMMERCE 24 (1998).

9 *See* Stender, *supra* note 5, at 293-94.

10 *See id.* at 294.

11 *Id.*

the process of converting ciphertext back into plaintext.[12] *Cryptographic systems* generally utilize a *cryptologic algorithm*, "a set of rules or series of mathematical steps," in conjunction with a *key*.[13] The *key* is usually a string of bits and is functionally analogous to a key that unlocks a door – it "unlocks" or decrypts the message so that the intended recipient can read it.[14]

There are two main types of key-based algorithms: *secret-key* (symmetric) and *public-key* (asymmetric).[15] In secret-key cryptographic systems, both the encryption key and decryption key are the same so that everyone who needs to decrypt the message must have the key distributed to them.[16] The inherent weakness in a secret-key system is "the problem of finding a trusted method to distribute the key, and moreover, protecting the key while in custody."[17] This type of scheme, however, is not practical for widespread commercial or personal use.[18]

In public-key cryptographic systems, the key used for encryption is different from the key used for decryption.[19] Consequently, this type of system "allows users to openly publish one key in the phone-book like directory (the 'public key'), while keeping the other key private (the 'private key')."[20] Public-key encryption "allows parties to exchange encrypted messages by using and revealing only their public keys, without ever having to exchange private keys."[21] As long as the recipient himself keeps secret the private key that matches the public key, only he can read messages encrypted with the public key."[22]

II. CURRENT REGULATIONS, PROPOSALS, AND INTERNATIONAL AGREEMENTS

A. EXPORT REGULATIONS

Currently, all exports from the United States are regulated under either the Arms Export Control Act ("AECA")[23] or the Export Adminis-

---

12 *Id.*

13 *Id.*

14 *See* BAKER & HURST, *supra* note 8, at 4.

15 *See* Stender, *supra* note 5, at 295.

16 *See id.*

17 *Id.*

18 This is because where there is no secure channel for exchanging the secret keys. Thus, the key exchange is subject to easy interception. *See* Ira S. Rubenstein, *Export Controls on Encryption Software*, in COPING WITH U.S. EXPORT CONTROLS 1994, at 183 (PLI Com. L. & Practice Course, Handbook Series No. A-705, 1994).

19 *See* Stender, *supra* note 5, at 296.

20 Rubenstein, *supra* note 18, at 183.

21 Stender, *supra* note 5, at 296.

22 BAKER & HURST, *supra* note 8, at 2.

23 22 U.S.C. §§ 2571-2794 (1994 & Supp. V. 1999).

tration Act ("EAA").[24] The AECA confers on the State Department the authority to regulate the export of anything it deems to be a munition, which it defines as "a weapon of war."[25] Items classified as munitions require individually approved export licenses which designate the customer, the application, and conditions for the handling or redeployment of the item.[26] If the State Department decides that an item is dual-use, a category that includes commercial products with military applications, it transfers jurisdiction over the item's export to the Department of Commerce ("DOC").[27] The DOC, under the EAA, now regulates the export of all encryption devices and software, except for those that are specifically designed or modified for military use.[28]

The DOC's Export Administration Regulations ("EAR")[29] define 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."[30] The EAR additionally define "exportation of encryption source code and object code"[31] as "[d]ownloading, or causing the downloading of, such software to locations . . . outside the U.S., or making such software available for transfer outside the U.S., . . . including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites."[32]

The Clinton administration initially instituted a restrictive encryption export policy over the objection of encryption software developers, who argued that such restraints would place an unnecessary burden on their ability to compete in the international encryption market.[33] However, on September 16, 1999, the Clinton administration announced that

---

24 50 U.S.C. app. §§ 2401-2420 (1994 & Supp. V. 1999).

25 *Id.*

26 *See* BAKER & HURST, *supra* note 8, at 106.

27 *Id.* Prior to December 30, 1996, the State Department was responsible for regulating the export of most encryption products from the United States under the AECA and the International Traffic in Arms Regulations ("ITAR"). *Id.* at 23. Jurisdiction over commercial encryption products was officially transferred from the State Department to the Commerce pursuant to Executive Order No. 13026 (Nov. 15, 1996). *Id.*

28 *Id.* at 24. Other agencies, including the Departments of Justice, State, and Defense, also have a say in decisions concerning commercial encryption exports. *Id.* The NSA, a division of the Department of Defense, has the most expertise in encryption matters. *Id.* Consequently, other agencies have usually deferred to the agency of the NSA on encryption export decisions. *Id.*

29 15 C.F.R. pts. 730-774 (2000).

30 *Id.* § 734.2(b)(1) (2000).

31 *Source code* refers to the text of a computer program written in a high-level programming language, such as *C* or *Pascal*. A computer cannot make use of source code until its has been translated into a lower-level, machine language, known as *object code*.

32 15 C.F.R. § 734.2(b)(9)(ii) (2000).

33 *See* Mai-Tram B. Dinh, *The U.S. Encryption Export Policy: Taking the Byte Out of the Debate*, 7 MINN. J. GLOBAL TRADE 375, 375 (1998) (The U.S. government has traditionally imposed restrictions on the export of encryption software in order to protect national security.).

the licensing requirements implemented by the Bureau of Export Administration ("BXA")[34] two years earlier would be changed so that the government allowed, after a one-time review, the marketing and export of 56-bit encryption technology, as opposed to the prior limit of 40-bit technology.[35] Moreover, the Administration eliminated the requirement that these software companies create and implement a key recovery system.[36] The Administration also directed "all executive departments and agencies to promote efforts domestically and internationally to make the Internet a secure environment for commerce."[37] The apparent rationale for this policy is that "encryption policy should align itself with market forces," because the mass use of encryption technology in the area of Internet technology is in the national interest.[38]

---

[34] The Bureau of Export Administration ("BXA"), a division of the Department of Commerce, has regulatory jurisdiction over encryption items and activities that are subject to the EAR. 15 C.F.R. § 734.2(a)(1). A BXA license or license exception is required for exports to all destinations, except Canada, for items controlled under Export Control Classification Numbers (ECCNs) which are designated as "encryption items." *Id.* pt. 774, Supp. No. 1. Such encryption items include "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR." *Id.* § 772.1. Encryption software includes "computer programs that provide capability of encryption functions or confidentiality of information or information systems," which includes "source code, object code, application software, or systems software." *Id.*

[35] *See* White, *supra* note 6, at 200-01. On September 16, 1999, President Clinton submitted to Congress a very general proposal entitled the Cyberspace Electronic Security Act of 1999 ("CESA"), which would purportedly "protect the growing use of encryption for the legitimate protection of privacy and confidentiality by businesses and individuals, while helping law enforcement obtain evidence to investigate and prosecute criminals despite their use of encryption to hide criminal activity." Press Release, Office of the White House Press Secretary, Cyberspace Electronic Security Act of 1999, Sept. 16, 1999) [hereinafter CESA], *available at* http://www.cdt.org/crypto/CESA/CESA revfactsheet2.shtml (last visited Feb. 23, 2000). CESA would allow law enforcement to maintain its ability to access decryption keys stored with trusted third parties, who protect such information from inappropriate release. *Id.* In addition, CESA would authorize "$80 million over four years for the FBI's Technical Support Center to serve as a centralized resource for Federal, State, and local law enforcement in responding to the increasing use of encryption by criminals." *Id.* CESA would not regulate the domestic development, use or sale of encryption, and Americans will remain free to use any encryption system domestically. *Id.* Under CESA, individuals would remain completely free not to use the services of a recovery agent. *Id.* CESA, however, remained noticeably silent regarding the exportation of encryption, so it was unclear whether "individuals" would include users of exported encryption \in addition to domestic users.

[36] *See* White, *supra* note 6, at 201.

[37] *Id.* at 202.

[38] *See id.; see also* Dinh, *supra* note 33, at 391 (explaining that, at an industry conference on the future of information technology, panelists representing the Federal Trade Commission and the National Computer Security Association agreed that "the success of e-commerce depends on consumers' confidence in the system and their belief that transactions are safe from meddlers"). However, critics of these amended export regulations pointed out that, given the wide availability of stronger 64 to 128-bit encryption products, foreign customers would reject American "encryption lite" products. *See* ACP, *supra* note 3. According to banking and computer executives, "40-bit codes are no longer safe and can be cracked in as little as a few hours by skilled computer hackers. The minimum acceptable code, according to

On January 14, 2000 the Clinton administration formally liberalized its licensing requirements on the export of encryption software products.[39] The new regulations[40] "allow United States companies to ship any retail encryption[41] products around the world to commercial concerns, individuals and other nongovernment users after a one-time technical review by an interagency panel."[42] In addition, the rules allow the export, without licenses, of most types of source code (the computer code used to create programs).[43] The only exceptions to these rules would be to nations on the State Department's list of seven terrorist supporting countries, which are Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.[44]

The new regulations amend the EAR to allow export of any encryption software or commodity to individuals, commercial firms, and other non-governmental end-users in all destinations, while more liberally allowing exports of retail encryption commodities and software to all end-users in all destinations.[45] In essence, the amended regulations implement the encryption policy announced by the White House on September 16, 1999, which rested on three principles: (1) technical review of encryption products in advance of sale, (2) a streamlined post-export reporting system, and (3) a process that permits the government to review export of strong encryption to foreign governments.[46] Cisco Systems, one of the largest producers of routers that form the backbone of the Internet, expressed modest enthusiasm for the new rules.[47] While Cisco

---

many bank executives, must have keys that are 128-bits long." Edmund Andrews, *U.S. Restrictions on Exports Aid German Software Maker*, N.Y. TIMES, Apr. 7, 1997, at D1.

39 *See* David E. Sanger & Jeri Clausing, *U.S. Removes More Limits on Encryption*, N.Y. TIMES, Jan. 13, 2000, at C1.

40 The new regulations essentially eliminate licensing requirements for strong encryption. But most products will still be subject to a one-time government review and companies are supposed to track and report their sales. *Id.*

41 Retail encryption commodities and software are "those which are widely available and can be exported and re-exported to any end-user (including any Internet and telecommunications service provider) to provide products and services (e.g. e-commerce, client-server applications, or software subscriptions) to any end-user." Revisions to Encryption Items, 65 Fed. Reg. 2493 (2000) (interim final rule at 15 C.F.R. pts. 734, 740, *et al.*) [hereinafter Encryption Items]. The criteria for determining whether something qualifies as a retail product includes

> functionality, sales volume, distributions methods, ability to modify products and requirements for substantial support by the supplier . . . . Finance-specific, 56-bit non-mass market products with a key exchange greater than 512 bits and up to 1024 bits, network-based applications and other products which are functionally equivalent to retail products are considered retail products.

Id.

42 Sanger & Clausing, *supra* note 39, at C1.

43 *Id.*

44 *Id.*; *see also* Encryption Items, *supra* note 41, at 2492.

45 *See* Encryption Items, *supra* note 41, at 2492.

46 *Id.*

47 *See* Sanger & Clausing, *supra* note 39, at C1.

and numerous other high-tech companies viewed the new regulations as a step in the right direction and "as delivering on Vice President Al Gore's promises to eliminate cumbersome licensing rules on exporting software, civil libertarians say they fail to fix the constitutional questions at the heart of pending court cases."[48]

B. LEGISLATIVE PROPOSALS

There have been three bills relating to the issue of encryption introduced during the 106th Congress, but only two of the bills specifically propose amendments to government regulation of encryption exports.[49] The Security and Freedom Through Encryption Act ("SAFE"),[50] proposes a less restrictive approach to export regulations that would allow U.S. companies to export strong encryption products if comparable products were already available overseas.[51] SAFE would remove existing export controls on hardware and software encryption products that are of comparable strength to those that are commercially available from a foreign supplier, regardless of any adverse impact on national security.[52] SAFE would also place a prohibition on any type of mandatory key recovery encryption by the government, but includes a provision that might make it criminal to use encryption in furtherance of a criminal act.[53] At the time of this bill's introduction, it enjoyed over 200 bipartisan co-sponsors.[54] The number of co-sponsors has grown to over 250 since that time.[55] As of late July 1999, the House Rules Committee was preparing to decide which version of SAFE should be sent to the House for a floor vote.[56]

The other congressional bill that addresses encryption export regulations is S.798, entitled the Promote Reliable On-Line Transactions to Encourage Commerce and Trade Act of 1999 ("PROTECT"), introduced by

---

48 *Id.*

49 FBI REPORT, *supra* note 1, at 10-13. The Electronic Rights (E-Rights) for the 21st Century Act (S.854), introduced Senator Leahy (D-VT) on April 21, 1999, proposes to "protect the privacy and constitutional rights of Americans, to establish standards and procedures regarding law enforcement access to location information, . . . to affirm the rights of Americans to use and sell encryption as a tool for protecting their online privacy . . . ." *Id.*

50 H.R. 850, 106th Cong. (1999). This bill was introduced Representative Robert Goodlatte (R-VA) on February 25, 1999. *See* FBI REPORT, *supra* note 1, at 10.

51 The computer industry, seeking an open world market for its encryption products, has long complained that such export restrictions are pointless because terrorists can simply buy powerful encryption products from other countries, such as Canada, Israel, or Ireland. *See Demos to Prez: 'Use SAFE Text,' at* http://www.wired.com/news/news/politics/story/21744.html (last visited March 17, 2001).

52 *See* FBI REPORT, *supra* note 1, at 11.

53 *See id.*

54 *See id.*

55 *See id.*

56 *See id.*

Senator John McCain (R-AZ) on April 14, 1999.[57] This bill calls for the relaxation of encryption export controls for certain sectors and "responsible" governments, while at the same time maintaining national security interests.[58] Under PROTECT, responsible governments include those of member nations of NATO, Association of Southeast Asian Nations, and the Organization for Economic Cooperation and Development.[59] PROTECT would also create an Encryption Export Advisory Board which would be responsible for keeping the Secretary of Commerce abreast on the latest encryption products that are available or will be available within twelve months from a foreign supplier.[60] This bill addresses NSA's concerns by including a provision that allows the President to override any decision by the Encryption Export Advisory Board for national security purposes.[61] PROTECT would also maintain presidential authority to prohibit the export of encryption products to countries that support terrorism or otherwise pose a threat to national security.[62]

C. INTERNATIONAL AGREEMENTS

The Wassenaar Arrangement, which "was set up as a multilateral export-control group that was designed to promote communication and cooperation in controlling dual-use goods, including cryptography," underwent a major change on December 3, 1998.[63] The thirty-three countries that subscribe to this Arrangement agreed "(1) to impose export controls on encryption software using keys above 64-bits in length, and (2) to eliminate record keeping for low-level encryption."[64] This agreement, however, does not level the playing field of the global encryption market because many countries, including Israel, South Africa, India, and China are not Wassenaar members.[65] Additionally, "while [this] agreement suggests a ceiling, it does not prevent member-countries from imposing stricter controls on encryption exports, as the United States has done."[66] The Clinton administration cited the amended Wassenaar con-

---

57 *See id.* at 12-13 (PROTECT is a pro-industry bill even though its stated purpose is "to promote electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protections of national security and other purposes.").

58 *See id.*

59 *See id.*

60 *See id.*

61 *See id.*

62 *See id.*

63 Staci I. Levin, *Who Are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls*, 30 LAW & POL'Y INT'L BUS. 529, 537 (1999).

64 *Id.*

65 *Id.*

66 *Id.*; *see also* F. Lynn McNulty, *Encryption's Importance to Economic Infrastructure Security*, 9 DUKE J. COMP. & INT'L L. 427, 435 (1999). The article states:

> The Wassanaar countries extended the group's Dual-Use Control List to encryption hardware and software cryptography products above 56-bits, which include web

trols to support its efforts to extend its levels of control on the export of cryptography.[67]

Prior to the January 14, 2000 amendment to the encryption export regulations, the American Electronics Association ("AEA"), an industry group representing 3,000 plus U.S.-based technology companies, supported "the Clinton administration's decision to align the U.S. export regulations with the new Wassenaar requirements and to deregulate products up to 56-bits, but [felt] the response [was] inadequate."[68] The AEA pointed out the folly of arbitrary line drawing since law enforcement and intelligence agencies find it no more difficult to break 65-bit than 64-bit encryption.[69] Critics suggested that the government reconsider whether its export policy can actually achieve its stated goals before trying to appease both the software industry and law enforcement officials by merely tinkering with the numbers and details.[70] The fact that the most recent encryption regulations impose no encryption key length limit for retail encryption products suggests that these critics' suggestions did not fall on deaf ears.[71]

III. EVOLUTION OF ENCRYPTION POLICY

A. HISTORICAL PERSPECTIVE

In assessing the arguments for and against the widespread availability of cryptography that would result from unregulated export, it helps to examine the development and application of cryptography. World War I was the first war to be fought in the era of radio, which made it possible to transmit and receive human voices over long distances.[72] The solution to the ubiquitous nature of radio reception, which enabled anybody with the right equipment and know-how to listen in, was cryptography. After WWI, the United States continued to develop its capacity for signals intelligence and merged this responsibility with the development of codes to protect U.S. military communications.[73] World War II was a triumph for American communications intelligence, which made important con-

---

browsers, e-mail applications, electronic commerce servers, and telephone scrambling devices . . . . [Member countries] also re-imposed controls on other mass-market products with strengths over 64-bits, such as personal computer operating systems, word processing, and data base programs.

Id.

67 *See* McNulty, *supra* note 66, at 436.

68 *Id.* at 436-37.

69 *See id.* at 437.

70 *See* 144 Cong. Rec. S12,151 at 12,152 (Oct. 9, 1998).

71 *See* Encryption Items, *supra* note 41, at 2492.

72 *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 49 (1998).

73 *See id.* at 52.

tributions to victories in both the Atlantic and Pacific:[74] "The Allies' ability to understand German and Japanese communications, even when they were encoded with the enemies' best cryptographic systems, is widely seen as having been crucial to the course of World War II."[75]

In 1952, President Harry Truman signed a secret presidential order creating the National Security Agency ("NSA"), whose objective was to "capture control of all cryptographic and cryptanalytic work within the United States."[76] During the 1970s, the NSA recognized that implementation of federal laws like the Family Educational and Privacy Rights Act of 1974,[77] combined with the increasing use of computers and digital communications by the federal government, would require that it share its cryptographic equipment with a wider range of government users.[78] Any cryptographic equipment that was to be put in the hands of users who did not undergo security clearance would have to utilize unclassified cryptographic algorithms.[79] The NSA feared that making any of its algorithms public would reveal information about its design philosophy and approach, which could conceivably compromise its other equipment.[80] During the late 1970s and 1980s, the NSA took notice of increased civilian research in cryptography and tried unsuccessfully to limit civilian development and application of this technology.[81] In the early 1990s, the FBI "formulated a policy that included shoring up its ability to perform electronic surveillance, . . . and preventing the establishment of unbreakable cryptography in the public sector."[82] The FBI's initial efforts in support of this policy were embodied in the concept known as *key escrow*.

B. THE RISE AND FALL OF KEY ESCROW?

Key escrow, later euphemistically renamed *key recovery* and *key management* in order to appease the fears of privacy advocates, is a system by which users of cryptographic equipment are able to protect their privacy against most intruders while allowing the government to keep a set of "spare keys" with which it can decipher and read the communica-

---

74 *See id.* at 53.

75 *Id.* at 6. During WWI and WWII the U.S. primarily implemented mechanical cryptographic systems, devices utilizing physical moving parts rather than electronic and magnetic components. *See id.* at 19-29. Since the 1940s, the U.S. has converted to purely electronic encryption. *See id.*

76 *Id.* at 55.

77 20 U.S.C. § 1232g (1994 & Supp. V. 1999).

78 DIFFIE & LANDAU, *supra* note 72, at 59.

79 *See id.*

80 *See id.*

81 *See id.* at 60-76.

82 *Id.* at 76.

tions.[83] Under this system, encryption keys are kept "in escrow" by a trusted third party.[84] These keys can only be released to "authorized parties, either predetermined or by court order."[85] The FBI claims that the use of trusted third parties to hold keys in escrow would have the benefit of providing assurance to "commercial and individual users of encryption that their encrypted communications and electronically stored information are secure against unauthorized disclosure and illegal 'hacker-type' attacks."[86]

The first proposed key escrow scheme, made public on April 16, 1993, was the Clipper Chip program, which allowed government officials to decipher messages for law enforcement and national security purposes.[87] Encryption businesses objected to the Clipper Chip program on the grounds that the added manufacturing costs, which would ultimately be passed on to the customer, combined with the existence of a "back door" made it unlikely that Clipper Chip products would appeal to foreign customers.[88] Critics of key recovery systems point out that "knowledge that the government has the technical ability to read all communications creates a perception that no communication is private, *even if* the vast majority of communications are never intercepted or read."[89] Americans for Computer Privacy ("ACP"), a broad-based coalition which primarily represents financial services, manufacturing, telecommunications, and high-tech groups, points out that the implementation of a mandatory key recovery system would have the effect of giving the FBI "immediate access to the plaintext of encrypted communications or electronic communication without the knowledge or cooperation of the person using such product or service."[90]

Despite industry-wide opposition to any sort of key recovery scheme, this type of system, currently referred to as Key Management Infrastructure ("KMI"), continued to exist within the Clinton administration's encryption export regulations.[91] However, this type of regulatory system seems to have lost any bite that it might have had as the Commerce Department has continued to issue an increasing number of license exceptions allowing merchants to export strong encryption after a one-

---

[83] *Id.* at 7.

[84] *See* Stender, *supra* note 5, at 298.

[85] *Id.*

[86] FBI REPORT, *supra* note 1, at 9.

[87] DIFFIE & LANDAU, *supra* note 72, at 7.

[88] *See id.*

[89] *See id.* at 212 (emphasis added).

[90] ACP, *supra* note 3, *at* http://www.computerprivacy.org/myths/ (last visited September 28, 2000).

[91] *See generally* Key Management Infrastructure (KMI), 15 C.F.R. § 740.8 (2000).

time technical review.[92] For example, under Encryption Licensing Arrangements ("ELAs"), distributors can export encryption goods "as long as they comply with restrictions contained in the ELA."[93] It appears that ELAs will vary on a case-by-case technical review basis, which suggests that there is no longer a uniform mandate requiring all encryption exporters to participate in any key recovery system.

IV. REGULATION OF ENCRYPTION EXPORTS PASSES CONSTITUTIONAL MUSTER

A. FIRST AMENDMENT ANALYSIS

In assessing whether governmental regulation of the export of encryption software raises First Amendment concerns, it is necessary to address two sub-issues. The first sub-issue is whether encryption software source code qualifies as "speech" for First Amendment purposes.[94] The second sub-issue is whether current U.S. export regulations are a prior restraint on speech.[95]

Of the two cases that have addressed the issue of whether source code is "speech," *Bernstein v. U.S. Dept. of Justice ("Bernstein III")*,[96] has received the most extensive judicial review. The three-judge panel of the Ninth Circuit ruled 2-1 in May 1999 that encryption program source codes contain expressions of ideas that cannot be suppressed by government officials.[97] Bernstein, a mathematics professor, sought to export to the international academic and scientific communities an encryption method, which he had developed during his days as a graduate

---

92 *Id. See also* Christopher R. Wall & Thomas M. DeButts, *Encryption Export Controls, in* COPING WITH U.S. EXPORT CONTROLS 1999 at 549,o55ϕ (PLI Com. L. & Practice Course, Handbook Series No. A0-002Q, 1999). Certain "encryption items," as defined in EAR, 15 C.F.R. pt. 772, may be exported under License Exception KMI (15 C.F.R § 740.8) after a one-time technical review by BXA. *Id.* Commodities and software eligible for the this License Exception KMI include "those for which companies had developed schemes for U.S. Government key recovery or deposit of keys with a key escrow agent under earlier encryption export control regimes. *Id.* However, recoverable commodities and software, as defined in EAR, 15 C.F.R. pt. 772, may also be exported pursuant to an encryption licensing arrangement ("ELA") when License Exception KMI cannot be used. 15 C.F.R. §§ 742.ϕ5(b)(2), 740.8. The effect of these licensing exceptions is to allow encryption commodities and software of any key length to be exported under a license exception to non-government end users in any country, except one of the seven designated terrorist countries. Wall & DeButts, *supra*. In addition, retail encryption commodities and software of any key length may be exported under a license exception to any country except the seven designated terrorist countries after a one-time technical review. *Id.*

93 Encryption Items, *supra* note 41, at 2492.

94 *See generally* U.S. CONST. amend. I.

95 *See* Bernstein v. U.S. Dept. of Justice, 176 F.3d 1132, 1138 (9th Circ. 1999) [hereinafter *Bernstein III*] (pointing out that "any prior restraint on expression comes . . . with a heavy presumption against its constitutional validity").

96 *Id.*

97 *Id.*

student.[98] The State Department classified the software, which utilized his encryption scheme, as a munition and told Bernstein that he would need a license to export the computer program.[99] In granting summary judgment for Bernstein, the district court found that the program's source code to be "speech" protected by the First Amendment.[100]

In December 1996, President Clinton shifted licensing authority for nonmilitary encryption commodities and technologies from the State Department to the Department of Commerce, which promulgated the EAR to govern the export of crypto.[101] Bernstein amended his complaint by adding the Department of Commerce as a defendant and advanced the same constitutional objections.[102] The district court again granted summary judgment for Bernstein, finding the EAR to be facially invalid as a prior restraint on speech.[103]

In affirming *Bernstein I* and *II*, the Ninth Circuit reasoned that cryptographers use source code to express their scientific ideas in the same way that mathematicians use equations or economists use graphs to express their findings or ideas.[104] The court seemed to emphasize the fact that *source code*,[105] unlike *object code*,[106] "is not meant solely for the computer, but is rather written in a language intended also for human analysis and understanding."[107] The circuit court's emphasis on the distinction between object code and source code is overly simplistic because source code is not necessarily intended for others to analyze or understand. Programmers who intend their source code to be understood by others usually include annotations and remarks throughout the program, whereas programmers who are more interested in the functionality or efficiency of their source code will be less inclined to include such descriptive annotations.

According to the standard set forth by the Supreme Court of the United States, the dispositive factor in determining "speech" for First

---

98 Bernstein argued he wanted to export his encryption methods for purely academic rather than commercial purposes. *See id.* at 1136. Bernstein's motive exporting encryption, however, is not dispositive on the issue of whether or not encryption software source code qualifies as "speech" under the First Amendment.

99 *Id.* at 1136.

100 *See* Bernstein v. U.S. Dept. of State, 922 F.Supp. 1426, 1434-36 (N.D. Cal 1996) [hereinafter *Bernstein I*].

101 *See Bernstein III*, 176 F.3d. at 1136.

102 *See id.*

103 *See id.*

104 *See id.* at 1141.

105 Source code refers to "text of a program written in a 'high-level' programming language, such as 'PASCAL' or 'C.'" *Id.* at 1140.

106 Object code refers to "lower-level" or "machine" language, which gives instruction to the computer. *See id.*

107 *Id.* at 1142.

Amendment purposes is whether it expresses ideas.[108] However, the Supreme Court has also pointed out that merely because something is occasionally expressive does not guarantee that the protections of the First Amendment extend to it.[109] In *Bernstein III*, the Ninth Circuit suggested that Bernstein's encryption method was intended, in part, as political expression of Bernstein's disagreement with US encryption exports regulations.[110] The assertion that this encryption program is political speech begs the question of who Bernstein's intended audience is. His audience, if it exists at all, would be limited to computer programmers who happen to be sifting through lines of code in search of a political message. This is not a common activity among programmers and people in general.

As Judge Nelson's dissenting opinion in *Bernstein III* pointed out, "while encryption source code may occasionally be used in an expressive manner, it is inherently a *functional* device."[111] The function of encryption source code is to render computer communication and transactions secret, thereby creating "a lockbox of sorts around a message that can only be unlocked by someone with a key."[112] The dissent also pointed out that "[i]t is the function or task encryption source code performs which creates its value in most cases. This functional aspect of encryption source code contains no expression . . e. ."[113] While encryption methods may be the subject of political or nonpolitical speech, it makes little sense to suggest that encryption source code qualifies as speech in and of itself. On September 30, 1999 the full court of the Ninth Circuit announced that a majority of its active judges had voted to grant the government's request for a rehearing, *en banc*, but no date has been set. In so doing, the court withdrew its *Bernstein III* decision.[114]

Junger v. Daley,[115] the other case which specifically addressed the issue of whether or not encryption source code should be considered "speech," held that encryption software source code is not sufficiently

---

108 *See* Roth v. U.S., 354 U.S. 476, 484 (1957); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976).

109 *See* City of Dallas v. Stranglin, 490 U.S. 12, 25 (1989) ("It is possible to find some kernel of expression in almost every activity – for example, walking down the street or meeting one's friends at the shopping mall – but such a kernel is not sufficient to bring the activity within the protection of the First Amendment.").

110 *Bernstein III*, 176 F.3d. at 1141 n.14.

111 *Id.* at 1148 (emphasis added).

112 *Id.*

113 *Id.*

114 192 F.3d 1308 (9th Circ. 1999).

115 Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998). Junger, a law professor at Case Western Reserve University who wished to post encryption programs on his web site, challenged the constitutionality of export regulations that prevented him from engaging in such activity. The court held that export of encryption software source code was not sufficiently expressive to receive First Amendment protection, and that export regulations requiring licensing of such software did not qualify as unconstitutional prior restraint.

expressive to merit First Amendment protection.[116] The district court reasoned that "speech" is protected not simply because it is written in a language but rather because it expresses ideas.[117] Encryption source code is rarely expressive, and in the limited instances it may communicate some idea, it is unintelligible to most people. That exporting source code may occasionally be expressive "does not necessarily extend First Amendment protection to it."[118]

According to *Karn v. U.S. Department of State*, even if one were to assume that encryption software source code qualifies as speech, export regulation of this software does not necessarily constitute a prior restraint on speech.[119] In order for an export licensing law to be invalidated by a prior restraint facial challenge, it "must have a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of . . . censorship risks."[120] If the export regulations are content-neutral[121] and aimed at preventing software exporters from making it easier for foreign intelligence sources to encrypt their communications, the government may justify such regulation if it: (1) is within the constitutional power of government, (2) furthers an important or substantial government interest, and (3) is narrowly tailored to the governmental interest.[122] Both the *Junger* and *Karn* courts applied this three-part test and concluded that U.S. export regulations were not a prior restraint on speech. As the *Junger* and *Karn* decisions and Judge Nelson's dissenting opinion in *Bernstein III* suggest, the First Amendment analysis weighs in favor of regulating the export of encryption software because its source code lacks substantial expressive value, and thus is not "speech" for First Amendment purposes.

B. FOURTH AMENDMENT ANALYSIS

The notion of informational privacy is implicit in the Fourth Amendment, which asserts "the right of the people to be secure in their

---

116 *Id.*

117 *Id.* at 717.

118 *Id.*; *see also* City of Dallas v. Stranglin, 490 U.S. 12, 25 (1989).

119 *See* Karn v. U.S. Dep't of State, 925 F.Supp. 1 (D.C. 1996) (holding that designation of the disk containing the encryption source codes as a "defense article" was not subject to judicial review; that export regulations did not violate Karn's First Amendment rights; and that export restrictions did not violate due process). This decision has subsequently been remanded to the district court to consider the constitutional effect of the transfer of jurisdiction of export controls from the State Department to the Commerce Department. *See* 107 F.3d 923 (D.C. Circ. 1997). However, it is unlikely that the First Amendment holding will be altered as a result of the change in governmental jurisdiction.

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

121 Content neutral regulations do not take into consideration what is expressed by the content of the regulated article or good. *See id.*

122 *See* United States v. O'Brien, 391 U.S. 367 (1968) (upholding the government's prohibition against burning draft cards and establishing the elements of prior restraint test).

persons, houses, papers, and effects."[123] Certain lobbying groups, such as Americans for Computer Privacy, favor lifting all controls on the export of encryption on the basis that government regulations and restrictions on encryption software will compromise the ability of individuals to secure the privacy of their e-mail.[124] Proponents for reducing encryption export restrictions also argue that the spread of stronger encryption tools will encourage worldwide adoption of more secure standards for ensuring privacy of communications. For example, businesses and their customers would have less fear that their credit card numbers or other private communications would be intercepted by third parties over the Internet. These privacy concerns, however, do not implicate the Fourth Amendment unless: (1) the consumer or end-user of the exported software has standing to bring suit against the United States for violating her Fourth Amendment privacy protections, and (2) the export regulations violate the consumer's reasonable expectation of privacy.[125]

The end-user of exported U.S. encryption goods will usually be an alien on foreign soil.[126] The Bill of Rights provisions of the U.S. Constitution, however, do not always extend to aliens, particularly when they are on foreign soil. The Fourth Amendment, for example, does not apply to searches or seizures conducted on foreign soil, even if the search involves agents of the U.S. government.[127] In other words, evidence obtained by foreign or U.S. officials from searches conducted in a foreign country is admissible in U.S. federal courts regardless of whether the search complied with the Fourth Amendment. The Fourth Amendment was not "understood by contemporaries of the Framers to apply to activities of the United States directed against aliens in foreign territory or in international waters."[128]

In the case of encryption export regulations, one might make the argument that violation of an end-user's expectation of privacy is violated within the U.S., in which case an alien end-user might have standing to bring suit against the U.S. It is difficult to pinpoint exactly where violation of the end-user's expectation of privacy occurs, assuming that

---

123 *See* U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347 (1967) (holding that citizens are entitled to a reasonable expectation of privacy).

124 *See* Jeri Clausing, *Concerns Raised Over Encryption Report*, N.Y. TIMES, Nov. 24, 1999, at C5.

125 *See* Terry v. Ohio, 392 U.S. 1 (1967) (adopting a sliding-scale reasonableness test for the individual's expectation of privacy).

126 An alien within the U.S. who wants to purchase encryption goods is not subject to EAR. *See* Encryption Items, *supra* note 41. Similarly, U.S. citizens and business wanting to use U.S. encryption devices are generally not subject to EAR. *Id.*

127 *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990); United States v. Behety, 32 F.3d 503, 510 (11th Cir. 1994); United States v. Cardenas, 9 F.3d 1139, 1157 n.8 (5th Cir. 1993).

128 *Verdugo-Urquidez*, 494 U.S. at 267.

there was indeed a violation of the end-user's reasonable expectation of privacy. However, the question of the territorial or geographic point at which the end-user's expectation of privacy was breached bears on the more general issue of whether this end-user would have standing to bring suit against the U.S. As the following analysis shows, even if the end-user or consumer of exported encryption has standing, current export regulations do not violate the consumer's reasonable expectation of privacy.

The Fourth Amendment doctrine has evolved as this country's technological developments have advanced. After the Supreme Court's decision in *Boyd v. U.S.*,[129] a search was considered unreasonable if the government's regulations intruded on an individual's private property rights without establishing a superior right vested in the property by the government. Utility, necessity, and significant public interest arguments by the government could not trump a citizen's property rights.

However, in the 1960s, the Supreme Court shifted the focus of the Fourth Amendment away from property rights in response to law enforcement's increased use of intrusive investigative techniques, such as wiretaps. The Court instead defined the limits of "search and seizure" in terms of whether the defendant displayed a subjective expectation of privacy and, in addition, whether the expectation was one society regarded as reasonable.[130] Search and seizure by the government was reasonable only if the government had probable cause and took the procedural step of obtaining a warrant.[131]

The Supreme Court again modified the Fourth Amendment doctrine in *Terry v. Ohio* by adopting a sliding-scale approach to measuring the reasonableness of a search and seizure.[132] Under this approach, the government is permitted to conduct a search and seizure based on a showing of reasonable suspicion.[133] The Court justified its departure from the probable cause requirement by accepting the government's argument that a limited search and seizure, such as in a stop and frisk,[134] is absolutely

---

129 116 U.S. 616 (1886).

130 *See* Katz v. United States, 389 U.S. 347 (1967) (holding that government's act of electronically listening to and recording defendant's words spoken into telephone receiver in public telephone booth violated the privacy upon which defendant justifiably relied while using the telephone booth).

131 *See id.*

132 *See* Terry v. Ohio, 392 U.S. 1, 27 (1967).

133 *Id.* at 27.

134 A stop and frisk is a situation where law enforcement officers who are suspicious of an individual run their hands lightly over the suspect's outer garments to determine if the person is carrying a concealed weapon. BLACK'S LAW DICTIONARY 1420 (6th ed. 1990). Also called a "pat down" or "threshold inquiry," a stop and frisk is intended to stop short of any activity that could be considered a violation of Fourth Amendment rights. *Id.* The scope of the search must be strictly tied to and justified by the circumstances which rendered the initiation of the stop. *Terry*, 392 U.S. at 18.

necessary for law enforcement.[135] The *Terry* approach to the Fourth Amendment has subsequently been expanded and applied to situations outside stop and frisk.[136]

Even if one were to assume that the end-user of the exported software has standing to bring a constitutionally-based suit against the United States, it would make little sense to apply the *Terry* analysis to encryption export regulations. The Fourth Amendment protects an individual's privacy from *affirmative* intrusions by the government, generally in the context of law enforcement activities.[137] The effect of an invasion upon a citizen's reasonable expectation of privacy is exclusion of the tainted evidence.[138] The exclusionary rule is intended to force law enforcement to disgorge evidence it has unlawfully obtained. In the context of crypto, protection of a consumer's Fourth Amendment privacy interest does not mandate in favor of wide dissemination of encryption technology since the consumer's Fourth Amendment privacy interest is not implicated until the government has affirmatively breached her reasonable expectation of privacy. Thus, even if the end-user or consumer of exported encryption has standing, refusing to allow exports of encryption technology does not constitute an invasion of this individual's expectation of privacy that would trigger Fourth Amendment analysis.

V. NATIONAL SECURITY CONCERNS

A. THE DILEMMA OF UNBREAKABLE ENCRYPTION

While the national security and law enforcement communities acknowledge that encryption has beneficial and legitimate uses, they are concerned "about the serious threat posed by the proliferation and use of robust encryption products that do not allow for the immediate, lawful access to the plaintext of encrypted, criminally-related communications and electronically stored data in accordance with strict legal requirements and procedures."[139] The rationale for the limits imposed by the Commerce Department on the export of strong encryption products is that such products might be used by hostile nationals or terrorists to hide

---

135 *See Terry*, 392 U.S. at 20.

136 Dena Klopfenstein, Comment, *Deciphering the Encryption Debate: A Constitutional Analysis of Current Regulations and a Prediction for the Future*, 48 EMORY L.J. 765, 801 (1999); *see, e.g.*, United States v. Mendenhall, 466 U.S. 544 (1980) (holding that persons suspected of carrying drugs could be stopped at the airport based only upon reasonable suspicion).

137 *See, e.g.*, United States v. White, 401 U.S. 745 (1971) (holding that a radio transmitter concealed on an informant to record and monitor conversations with defendant, without warrant, at defendant's home violated defendant's Fourth Amendment right to be secure against unreasonable searches and seizures); Katz v. United States, 389 U.S. 347 (1967).

138 *See* Mapp v. Ohio, 367 U.S. 643, 655-56 (1961) (articulating the exclusionary rule).

139 FBI REPORT, *supra* note 1, at 1.

their communications from U.S. intelligence agencies."[140] According to the FBI, "law enforcement continues to experience an increase in the number of encounters with, and the subsequent damaging and detrimental effects of, the use of commercially-available encryption by criminals, terrorists and in hostile intelligence activities throughout the United States and across international borders."[141]

The Clinton administration asserted that "[t]imely action against terrorists, drug dealers, or kidnappers may require rapid access to electronic information that must not be thwarted by encryption."[142] Rather than taking on the unnecessary and impossible task of eradicating strong crypto, the government has made it its objective to "prevent unbreakable encryption form becoming routine."[143] In a world where unbreakable encryption is commonplace, "[a]ll communications on the information highway would be immune from lawful interception. In a world threatened by international organized crime, terrorism, and rogue governments, this would be folly."[144]

According to Louis J. Freeh, Director of the FBI, the potential adverse impact on public safety and national security resulting from a "wait and see" approach is "too great to justify catering to the narrow interest of computer software companies."[145]

Even reducing the decoding time to days or weeks may not be sufficient to prevent the types of crime the export policy targets. Legally authorized wiretaps generally provide crucial information just before a crime is to occur; similarly, a nearly instantaneous ability to decode messages is necessary to prevent crimes on the Internet. Effective law enforcement depends on electronic surveillance and search and seizure."[146]

---

140 *See generally id.*

141 FBI REPORT, *supra* note 1, at 6 (The Aldrich Ames and Ramzi Yousef cases are often cited to illustrate use of encryption technology by criminals to conceal their activity.); *see* White, *supra* note 6, at 198. In the Aldrich Ames spy case, "Ames was told by his Soviet handlers to encrypt computer file information to be passed to them." FBI REPORT, *supra* note 1, at 5. Similarly, Ramzi Yousef's terrorist plan to blow up eleven U.S. owned airlines in the Far East was found in encrypted computer files in Manila after his arrest. *Id.* Incidentally, Yousef was also the mastermind behind the bombing of the World Trade Center. *Id.*

142 CESA, *supra* note 35, at 1.

143 Steven Levy, *The Cypherpunks vs. Uncle Sam*, N.Y. TIMES, June 12, 1994, § 6 (Magazine), at 43.

144 Dorothy E. Denning, *The Clipper Chip Will Block Crime*, NEWSDAY, Feb. 22, 1994, at 35. Denning is a Georgetown University computer scientist who regularly contributes to the encryption debate.

145 *The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry: Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the Senate Comm. on the Judiciary*, 105th Cong. 43-46 (1997) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

146 Dinh, *supra* note 33, at 392-93.

The traditional line between "law enforcement" and the "intelligence community" has been blurred since the end of the Cold War.[147] The ability of the NSA, the primary agency charged with the collection of foreign signals intelligence, to intercept and exploit such signals is fundamental and necessary to U.S. security.[148] The inability to decrypt scrambled communications would greatly diminish the value of the NSA's signals intelligence activities.[149]

Cryptology is crucial for the intelligence community's ability to meet the arising challenges in the post-Cold War world, which includes "the proliferation of weapons of mass destruction, terrorism, narcotics-trafficking, and economic competitiveness."[150] U.S. intelligence activities, through and including the Persian Gulf War, provide numerous instances in which the intelligence community's cryptanalytic skills proved crucial to the success of U.S. military operations.[151] Nevertheless, there are those who completely oppose any form of U.S. intelligence operations, even at the cost of national security. For example, a group referring to themselves as techno-anarchists advocates "a Brave New World in which governments disintegrate and individuals from the nucleus of society . . . ."[152] Techno-anarchists believe that unbreakable encryption will empower individuals by making it "impossible for governments to control information, compile dossiers, conduct wiretaps, regulate economic arrangements, and even collect taxes."[153] Interestingly, the leader of this techno-anarchist movement, Timothy May, both acknowledges and embraces the potential danger of widespread availability of unbreakable crypto.[154]

B. DOES THE PROLIFERATION OF STRONG ENCRYPTION ADVANCE NATIONAL SECURITY INTERESTS?

Some scholars fear that widespread use of unbreakable encryption will have the effect of converting computers and telecommunications systems into "safe havens for criminal activity . . . [providing] a means for tax evasion, money laundering, espionage, contract killings, and implementation of data havens for storing and marketing illegal or controversial material."[155] Americans for Computer Privacy, on the other hand, argues that any U.S. export restrictions will be detrimental to both

147 *See* Stender, *supra* note 5 at 326.
148 *See id.* at 327.
149 *Id.* at 328.
150 *Id.*
151 *See id.* at 328.
152 *Id.* at 334.
153 *Id.*
154 *Id.* at 334-35.
155 *Id.*

the national security interests and businesses of the United States.[156] There seem to be two competing approaches to looking at the connection between encryption and export controls: (1) that wide availability and implementation of strong encryption technology will provide a better way to protect highly confidential information,[157] and (2) that restriction of the availability of strong encryption will render it more difficult for dangerous individuals and groups to conceal activities which pose a serious threat to national security.[158]

With regard to the first approach, while worldwide availability of U.S. encryption products may help protect U.S. businesses and industries from computer crime, fraud, and theft, it is disingenuous to claim that U.S. national security interests will also be advanced by proliferating the global market with our more advanced encryption products *unless* everybody in the world, including criminals, terrorists, and other people with hostile agendas, agreed to store their encryption keys with a trusted third party or similar entity within a key recovery system. This scenario seems highly improbable in light of the fact that no global infrastructure exists to support key recovery.[159] In fact, many countries have already decided not to participate in the key recovery system.[160] Moreover, the ACP itself adamantly opposes any sort of mandatory key recovery system.[161]

The second approach, which asserts that restriction of the availability of strong encryption will make it harder for dangerous individuals to conceal their activities, will not be favorable to U.S. high-tech companies which hope to obtain their share of the millions of dollars that analysts predict will be made in the global encryption market.[162] This approach may help the national security cause at least with regard to U.S. strong encryption technology, because those with hostile agendas will have to work a little harder to acquire and implement strong encryption. The effectiveness of this approach will largely depend on availability of strong encryption from non-U.S. sources. If there is wide availability of such technology from foreign sources, then restrictions on the export of U.S. encryption technology may only marginally advance national security interests.

---

156 *See generally* ACP, *supra* note 3.

157 *See id.*

158 *See* FBI REPORT, *supra* note 1, at 1-2.

159 *See* ACP, *supra* note 3 (stating that "despite the Administration's best efforts over the years, not one bilateral or multilateral agreement has been reached regarding the global exchange of encryption keys").

160 *See id.*

161 *See generally id.*

162 *See infra* Part VII.B.

Even when one takes into consideration the fact that "a significant number of encryption programs are already available from non-U.S. sources worldwide, and in many cases obtained quite cheaply and easily, it would appear not to be in the best interests of the United States, as a pure security matter, to contribute to the proliferation of encryption."[163] This situation is consistent with the U.S. policy of restricting the export of other military-related technology, such as Patriot Missile Technology, available from foreign sources.[164] The United States does not allow the unbridled export of sophisticated missile technology, which obviously poses a threat to national security, merely because China and Russia have similar systems available.[165]

VI. ARGUMENTS FOR LIBERALIZING ENCRYPTION EXPORT REGULATIONS

A. INFEASIBILITY OF RESTRICTING EXPORT OF ENCRYPTION SOFTWARE AND GOODS

As the government suggests, the widespread availability of strong encryption technology to terrorist organizations or unfriendly foreign countries could compromise national security interests. However, limiting foreign availability of U.S. encryption technology is not the most effective way to protect our national security when one considers the fact that such technology is readily available from other countries. At a hearing on U.S. counter-terrorism policy before the Senate Judiciary Committee, Senator Sam Nunn stated that the U.S. cannot "limit the power of encryption successfully over the long term. That's like trying to limit technology. I do not think it can be done."[166]

Senator Nunn was right. For one, state-of-the-art, non-key recovery encryption is freely available from non-American multinational corporations like Siemens and Brokart.[167] Some foreign companies, prior to the January 2000 amendments to the EAR, have marketed their unrestricted

---

163 OFFICE OF TECH. ASSESSMENT, O.T.A.-ISS-596, U.S. CONG., EXPORT CONTROLS AND NONPROLIFERATION POLICY 56 (1994) (noting that arguing for decontrol of exports because they can be found elsewhere is analogous to allowing uncontrolled gun sales to criminals simply because they can get them anyway).

164 *See also* Stender, *supra* note 5, at 322, 337 (Export controls have the effect of limiting the availability of U.S. crypto, much like export controls which "limit the availability of Patriot Missile technology despite similar systems being available to one degree or another worldwide.").

165 *See id.* Because strong encryption can easily be applied in a manner which harms our national security, it can arguably still be considered a potential munition, sometimes referred to as a dual-use item. Making potential foreign criminals and terrorists "work harder" to get this potential munition could be seen as advancing national security interests.

166 *U.S. Counter-Terrorism Policy: Hearing Before the Senate Judiciary Committee*, Federal News Service, Sept. 3, 1998.

167 *See* ACP, *supra* note 3; *see also* Andrews, *supra* note 38, at D1.

products as "stronger security than any U.S. company can provide."[168] In addition, the mathematical algorithms and formulas which provide the basis and foundation for advanced encryption technology are readily available over the Internet.[169] Critics of the earlier and more restrictive encryption export regulations have pointed out that it makes little sense to restrict the export of this technology when the encryption genie is already out of the bottle.[170]

In addition, some U.S. companies have worked around U.S. encryption policies by forming foreign ventures, allowing them to develop, manufacture, and export strong encryption technology without regard to U.S. export policies.[171] Additionally, there are various ways of illegally distributing U.S. encryption technology. For example, there is a personal use exemption that "allows U.S. citizens and permanents residents to travel abroad with encryption hardware and software."[172] While there are guidelines for travel with such equipment, there are no definitive means for determining if a product is illegally exported or not.[173] Additionally, modems allow for the illegal transmission of encryption software to parties in foreign countries.[174] The EAR itself permit encryption software to be placed on internet sites within the U.S. as long as the provider implements safeguards that are "adequate to prevent unauthorized transfer of such code outside of the United States."[175] These safeguards, however, will ultimately fail to keep encryption products away from foreigners because a "foreign person who has signed up for Internet access using a U.S. Internet Service Provider ('ISP') and who signed into the secure download site either from the United States or who paid long distance charges to dial-in to a U.S. ISP from an overseas location" would have access to this encryption software.[176]

Thus, critics of export controls point out that while the goal of encryption export regulations is to preserve national security, the "global availability of strong encryption software through foreign developers and the Internet will continue to thwart that goal, severely damaging the U.S.

---

168 Andrews, *supra* note 38, at D1.

169 *See id.*

170 *See id.*

171 Dan Goodwin, *True Tales from the Encrypt*, LEGAL TIMES, Apr. 21, 1997, at 2.

172 White, *supra* note 6, at 202.

173 *See id.*

174 *See id.*

175 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 (citing 15 C.F.R. § 734.2(b)(9)(ii) (1999)).

176 *Id.*

software industry at the same time."[177] Moreover, any individual engaged in serious criminal or terrorist activity who thinks that cryptography would further that activity is unlikely to be deterred from using homemade or underground products.

B. POTENTIAL ADVERSE ECONOMIC IMPACT OF RESTRICTIVE ENCRYPTION REGULATIONS

At a hearing of the 105th Congress in 1997 on the Security and Freedom Through Encryption Act ("SAFE"), William A. Reinsch, Undersecretary of Commerce for Export Administration, stated that "no empirical evidence supported the assertion that American firms are suffering grave losses because other countries do not restrict the export of encryption software."[178] Critics of the U.S. encryption export policies, past and present, however, point out that these policies, rather than having the intended effect of slowing down the spread of powerful encryption technology, created "a bonanza for alert entrepreneurs outside the United States" who carved out booming business by selling powerful encryption technology around the world that the U.S. government prohibited American companies from exporting.[179]

In 1997, software industry analysts estimated that U.S. encryption export policies placed domestic companies at risk of losing $60 billion in the global software market because competing international software companies had the opportunity to export much stronger encryption technology.[180] According to a 1999 report issued by the Economic Strategies Institute ("ESI"), "the U.S. economy could lose $97 billion over the next five years as a result of continued export controls on cryptographic products."[181] ESI's report also warned that American companies could lose an additional $140 billion in sales, because foreign consumers would be deterred from buying U.S. encryption products under the fear that the confidentiality of their e-mails and phone calls could be compromised by U.S. intelligence services.[182]

---

177 Levin, *supra* note 63, at 544; *see also* Stender, *supra* note 5, at 320-21 (stating that "criminals and spies have plenty of crypto available worldwide, and therefore there is simply no need to restrict U.S.-built crypto").

178 *The Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Telecomm., Trade, and Consumer Prot. of the House Comm. on Commerce*, 105th Cong. 56 (1997).

179 *See id.*

180 *See* Andrews, *supra* note 38, at D1 (reporting that Brokart Information Systems, a German software company, has profited by selling strong encryption software to companies like America Online, Netscape Communications, and Microsoft, because U.S. export regulations do not allow American companies to export powerful encryption technology).

181 McNulty, *supra* note 66, at 444 n.112 (citing Eric R. Olbeter, *Encryption and Security*, J. OF COM., Aug. 6, 1998, at 7A).

182 *See id.* at 444 n.113.

U.S. encryption export regulations have forced many U.S. companies to incur the costs of restructuring their computer software development departments, namely to develop multiple versions of their software – both a domestic version and an exportable version with weaker encryption.[183] Consequently, these companies had three alternatives in exporting computer software that uses encryption technology; they could: (1) export weaker versions of their software, (2) enforce an encryption key escrow system, or (3) develop alliances with foreign companies and produce encryption goods overseas.[184] Another way in which encryption export policy has cost the U.S. economy is the fact that U.S. software companies are forced to alter their production and marketing departments. For example, Netscape Communications must continually monitor its web site in order to prevent foreign users from downloading the "domestic", 128-bit version of its browser software.[185] In June 1998, several chief executive officers of the leading American computer firms formed the Business Software Alliance, which issued a report entitled "The Cost of Government-Driven Key Escrow Encryption."[186] This report concluded that "government plans to institute a federal key recovery/escrow infrastructure, designed to give law enforcement and intelligence agencies access to encrypted materials, would cost as much as $7.7 billion a year."[187]

VII. PROPOSED SOLUTION

A. FUNDING OF A CENTRALIZED COUNTER-ENCRYPTION RESEARCH AND DEVELOPMENT EFFORT THROUGH TAXATION OF ENCRYPTION EXPORTS

Any type of proposed solution to the encryption export debate will require a balanced approach that takes into consideration public safety and national security concerns while not unduly hindering the ability of the U.S. high-tech industry to compete in the global encryption products market. To this end, this note proposes that the U.S. government continue with its trend of easing encryption export restrictions, and in the place of licensing restrictions introduce a less burdensome "encryption

---

183 *See* Jeffrey H. Matsuura & George B. Delta, *Export Controls on the Internet*, J. PROPRIETARY RTS., Mar. 1998, at 2, 11.

184 Levin, *supra* note 63, at 543 (citing James J. Carter, Comment, *The Devil and Daniel Bernstein: Constitutional Flaws and Practical Fallacies in the Encryption Export Controls*, 76 OR. L. REV. 981 (1997)).

185 *See* John Simons & David Bank, *Restrictions are Relaxed on Encryption Exports*, WALL. ST. J., Sept. 17, 1998, at A3.

186 *See* McNulty, *supra* note 66, at 433. Member companies of the Business Software Alliance include Microsoft, Novell, Adobe, Bentley Systems, FileMaker, Lotus Development, Sybase, and Symantec. *See id.*

187 *Id.*

export tax" which would be used to fund the research and development of advanced decryption or counter-encryption[188] methods and tools by a centralized and joint effort of law enforcement and intelligence communities.

One compelling reason for such a proposal is the fact that licensing restrictions are not an effective way of ensuring our national security and cannot be a substitute for developing the technology and tools needed by law enforcement and the NSA officials to decrypt and obtain access to the plaintext information crucial to their respective functions. One way to ensure the national security of the United States in the digital information age is for the government to stay abreast of and in the forefront of the latest encryption technology. Controls on technology, regardless of how they are structured or enforced, cannot substitute for continuing technological advances by the United States.[189]

Governmental investment in the research and development in the area of cryptography may be the most feasible and reliable way to assist law enforcement and intelligence groups, and thus protect our national security interests, according to a report by the National Research Council ("NRC").[190] NRC's report suggests "that a technical center should be established to aid federal, state, and local officials burdened with the task of solving highly sophisticated technological problems."[191] The Clinton Administration has itself expressed support for "the creation of a *centralized* law enforcement resource within the FBI to provide law enforcement with urgently needed technical capabilities to fulfill its proliferation and use of strong, commercially-available encryption products . . . ."[192] The FBI currently has a Computer Analysis and Response Team ("CART"), which "is responsible for providing assistance in law enforcement investigations where computer generated and/or electronically stored information has been obtained pursuant to court authorized search and seizure."[193] The CART has witnessed "the number of cases utilizing encryption and/or password protection increase from two percent to approximately twenty percent over the past four years, to include the use of

---

188 From a theoretical standpoint, there appear to be two main ways of obtaining access to the plaintext of an encrypted message. The first approach would be a "brut-force" method of using an algorithm to try all the logically possible combinations until the encryption code is cracked. The second approach would be a "back door" method, which allows a person with knowledge of how the encryption program operates to somehow break into and manipulate the program itself to decipher the encrypted message.

189 *See* THEODORE J. ECKERT, THE TRANSFER OF U.S. TECHNOLOGY TO OTHER COUNTRIES: AN ANALYSIS OF EXPORT CONTROL POLICY AND SOME RECOMMENDATIONS 40 (1981).

190 *See* White, *supra* note 6, at 203 n.178.

191 *Id.* at 203 n.178.

192 FBI REPORT, *supra* note 1, at 10.

193 *Id.*

56-bit Data Encryption Standard and 128-bit Pretty Good Privacy encryption."[194] Even more,

> [t]hese totals are expected to increase significantly with the introduction of Microsoft's newest operating system, Windows 2000. This new operating system will allow users to employ an Encrypted File System ("EFS") which will provide the individual computer users with easy to use 'point and click' encryption thereby enabling the user, including criminals and terrorists, to easily encrypt all of the files stored on their computer.[195]

Some have pointed out that "[w]hile the NRC is very ambitious in its recommendation that the government direct its resources to the development of advanced counter-encryption technologies, that stance does not solve the government's need to protect national security interests *today*."[196] Even these critics, however, do not deny that it is important for law enforcement to develop the ability to descramble strong encryption codes. Rather, these critics point out that law enforcement *currently* lacks the ability to decipher information encoded with strong encryption, and thus argue that government officials should have some means of cracking encrypted information in legitimate law enforcement contexts.[197] As we move into the Information Age in the twenty-first century, it will be critical for us to ensure that law enforcement and intelligence officials have the tools and know-how to effectively carry out their respective functions.[198]

---

[194] *Id.* at 7. Pretty Good Privacy ("PGP") has "become the program of choice among longtime Internet users and technical wizards." Lisa Guernsey, *Secrecy for All, as Encryption Goes to Market*, N.Y. TIMES, May 18, 2000, at G1.

[195] FBI REPORT, *supra* note 1, at 7-8.

[196] Dinh, supra note 33, at 397 (1998). Dinh argues that while an encryption export policy requiring U.S. software vendors to provide the government with decryption keys or commit to providing such keys in the future may not be ideal, "no alternative achieves a better balance of interest in privacy, economic growth, and national security." *Id.* at 375. The NRC, however, flatly rejects a key management system as untested and instead emphasizes governmental investment in advanced counter-encryption technologies. The NRC is particularly concerned with the "uncertainty of market response to the aggressive promotion of escrow procedures." *Id.* at 392.

[197] *See id.* at 392-393. According to ACP, "[f]or today's commercially sold encryption products, [namely 128-bit encryption], the technology does not exist to provide immediate access to communication without the knowledge of the user." ACP, *supra* note 3. This would be like the "FBI mandating compact disk quality sound recording in the days of the 45-RPM record." *Id.*

[198] *See* Stender, *supra* note 5, at 320 (Law enforcement and national security intelligence argue that unbridled proliferation of strong encryption to criminals, terrorists, and foreign intelligence targets of interest will seriously undermine the government's ability to protect the security of state and its citizens.).

A large part of the purported detrimental effects to the computer and software industry that result from restrictions on encryption exports appears to be the loss of global market share.[199] These industries fear that they will lose their dominance in world markets "if offshore developers incorporate high-quality cryptography into their products while U.S. industry either cannot do so or suffers higher costs or delays due to requirements for export licenses because of strict controls of export of cryptography."[200] Prior to the January 2000 changes to U.S. export regulations, which lifted the limit on the strength of encryption exports, a reason for the imposition of a marginal encryption export tax in place of a burdensome encryption export licensing scheme might have been to avoid hamstringing U.S. high-tech companies from effectively competing in the global market, especially in light of the fact that non-American companies are not subject to encryption export restrictions.

Current U.S. encryption export regulations, however, are much less restrictive and friendlier to U.S. companies who want to ship their encryption products overseas. Still there are other policy reasons for imposing an encryption export tax. As stated earlier, the ability of the U.S. to stay abreast of the latest encryption is critical to the national security of our country in the digital information age. Funding for this endeavor has to come from somewhere. Who should pay for this? From a fairness standpoint, it seems that companies and individuals that stand to profit by exporting the strongest encryption products should have to contribute the most to counter-encryption research and development funds. Otherwise, exporters of encryption impose a negative externality[201] upon other U.S. citizens and corporations who do not export similar technology to foreign end-users.

The profit-driven activities of U.S. encryption exporters are likely to create new costs because law enforcement and intelligence agencies are placed in a situation in which they will have to invest more time and money in developing counter-encryption technologies. This type of situation might be characterized as a "commons dilemma" in that (1) we have a resource, namely national security, which is shared by multiple parties, and (2) those parties who compromise or "use up" this resource, namely exporters of encryption technology, do not absorb all of the costs of their activities.[202] The effect of such a situation is to encourage encryption exporters to over-utilize the U.S.'s national security re-

---

199 *See* McNulty, *supra* note 66, at 443-44.

200 Stender, *supra* note 5, at 321.

201 *See* STEPHEN G. BREYER ET AL., ADMINISTRATIVE LAW AND REGULATORY POLICY, PROBLEMS, TEXT, AND CASES 7 (4th ed. 1998).

202 *See generally* JEFFREY J. RACHLINSKI, MATERIAL FOR ENVIRONMENTAL LAW 87 (2000).

sources.[203] As this note proposes, one way to counter the profit-motivated incentive to over-utilize national security interests is to impose an encryption export tax. In summary, the rationale for imposing such a tax is two-fold: (1) the U.S. government will have to allocate a portion of its research and development funds toward counter-encryption technology in order to provide adequate national security in the digital information age; and (2) the negative externality costs associated with exporting encryption technology can be reduced by imposing a tax on U.S. distributors who plan to profit by exporting strong encryption technology.

Of course, any sort of encryption export tax should not be so burdensome that it drives U.S. companies out of the encryption industry or disrupts the financial stability of U.S. companies who decide to compete in the global encryption market. Imposition of a new tax in any given industry or market brings with it the possibility that some of the smaller competitors will be driven out of the market because they lack the financial resources to effectively compete with the bigger companies.[204] This scenario is not unique to the encryption market, and may be an associated cost that the U.S. must bear in implementing a more liberalized export policy. However, because the U.S. software companies control seventy-five percent of the global software market share, it is plausible that the U.S. software industry, unlike its foreign competitors, will be able to absorb the additional costs associated with an encryption export tax.[205]

Inevitably, privacy advocates, such as the Americans for Computer Privacy, would balk at the suggestion of supporting any type of governmental effort to develop counter-encryption devices and tools. Groups like the ACP would likely argue that such counter-encryption efforts could create the means for Big Brother[206] to monitor all private communications. Putting aside the issue of whether governmental counter-encryption efforts will transform our society into Orwell's futuristic nightmare, suffice it to say that the U.S. government will most likely invest in the development of counter-encryption technology, as will the private sector. By imposing an encryption export tax, the government would make sure that companies that stand to profit by exporting encryp-

---

[203] *See id.* at 89 (The underlying feature of the commons dilemma is that the parties in a position to use up a resource do not bear all of the costs of using up the resource.).

[204] The advancement of technology and new communications mediums through which companies can carry out their business transactions, such as the World Wide Web, may ultimately change the dynamics of competition between larger and smaller companies in a given market. For example, it is possible that the lower overhead costs of operating a web-based business may allow smaller, leaner companies to out savvy larger, sluggish competitors.

[205] *See* McNulty, *supra* note 66, at 781.

[206] *See generally* GEORGE ORWELL, 1984 (1st ed.) (1949).

tion software and devices contribute their fair and proportionate share into the U.S. counter-encryption development fund.

B. How Would the Proposed Tax Operate?

The proposed encryption export tax would operate on a sliding scale and vary depending on the strength of encryption incorporated into the exported product. For example, the tax rate would be higher for 512-bit than for 128-bit encryption technology. The rationale for this sliding scale is that stronger encryption exports create a greater negative externality in terms of national security. The proposed tax would not vary depending on which countries received the encryption products.[207] Varying the tax in this manner could have the effect of straining trade relations among countries or creating a scenario in which U.S. distributors export their goods to a country with a relatively lower tax rate only to have a distributor in that foreign country send their goods to end-users in other foreign countries, thereby circumventing higher export taxes. The specifics on what the tax rate should be for a given encryption strength is best left for the Department of Commerce to decide, since they are the best position to determine the tax rates which would best serve the goal of preventing the national security "commons dilemma" while not being overly burdensome on U.S. companies. Factors which the DOC should consider in determining tax rates include, but are not limited to, the strength of encryption and the availability of similar products from foreign distributors.

C. Which Agencies Would Be Responsible for Running the Fund? Where Would the Funds Go, and How Would They Be Used?

Under the proposed system, the DOC, which is currently responsible for regulating the export of all non-military use encryption devices,[208] would be the agency in charge of taxing U.S. distributors who wish to export encryption goods. There are a couple of different ways in which the DOC could carry out this function. DOC officials could conduct on-site visits and inspections for some of the larger companies wishing to export their encryption devices. Alternatively, the DOC could set up regional centers where smaller business operators could travel to undergo a review of the amount, types, and strength of encryption devices they want to export. The DOC could also require that all encryption exports go through its own customs officials for inspection and review of

---

207 The proposed tax would not alter the current EAR's prohibition on encryption exports to countries on the State Department's list of terrorist supporting countries. *See* Encryption Items, *supra* note 41, at 2492.

208 *See supra* text accompanying note 24.

the amount and strength of encryption goods sought to be exported. Because it is difficult to say which approach would be the most effective and efficient from an administrative standpoint, it would be best to defer to the DOC's decision on how to enforce and collect the encryption export tax.

The funds collected from this encryption export tax would ultimately go from the DOC to a centralized technical agency whose task it would be to develop advanced counter-encryption technologies and tools,[209] which would in turn be used to assist the law enforcement and intelligence agencies burdened with having to overcome highly sophisticated technological problems.[210] This note proposes that the government establish such a centralized technical agency, as the NRC has suggested, or that the FBI's CART and the NSA merge their efforts in developing counter-encryption technology. Revenue from the encryption tax would go directly from the DOC to the government's research and development fund. Alternatively, this revenue could take an indirect route by going from the DOC to the Department of Treasury, and from there to the government's counter-encryption research and development fund. This second approach might assist the Treasury Department in carrying out its function of collecting federal income taxes through the Internal Revenue Service. Once again, it would be best to defer to the DOC's judgment as to which procedures to implement in carrying out its function of collecting and distributing funds for the research and development of counter-encryption technology.

VIII. CONCLUSION

The justification and means for implementing governmental regulation of exportation of encryption technology should carefully weigh the policy interests advanced by all interested parties. The policies advanced by various groups, namely (1) U.S. high-tech industry advocates, (2) privacy advocates, and (3) national security advocates, in this debate are numerous and compelling. At the end of the day, however, the constitutionally based arguments for repealing current encryption export regulations, advanced primarily by privacy and some industry advocates are not persuasive. Instead, there are strong *economic incentives* for easing export regulation, as there are equally compelling *national security reasons* for maintaining some level of regulation. It would be difficult for anybody to argue that the extra profits to be reaped by certain companies and individuals in the encryption software industry outweigh the security of our nation as a whole.

---

209 *See supra* text accompanying note 188.

210 *See supra* Part VIII.A.

What is needed is a balanced approach to encryption export regulation which will best ensure our national security interests while not being overly burdensome on U.S. companies who wish to compete in the global encryption market. As stated previously, this note proposes that the U.S. government, in place of regulating through licensing restrictions, introduce a nominal "encryption export tax" which would be used to fund a joint and centralized effort by the FBI and NSA to research and develop advanced decryption technologies and tools. The proposed tax would make sure that the companies and individuals who stand to profit by exporting strong encryption products contribute their fair and proportionate share to the governmental counter-encryption research and development funds, which will in turn provide the tools needed to ensure our national security in the digital information age.