THE DILEMMA FOR FUTURE COMMUNICATION TECHNOLOGIES: HOW TO CONSTITUTIONALLY DRESS THE CRYPTO-GENIE[1]

Jason Kerben

> "The proliferation of encryption of technology threatens the ability of law enforcement and national security officials to protect the nation's citizens against terrorists, as well as organized criminals, drug traffickers and other violent criminals."[2]
>
> "If the freedom of the press . . . [or freedom of speech] perishes, it will not be by sudden death . . . It will be a long time dying from a debilitating disease caused by a series of erosive measures, each of which, if examined singly, would have a great deal to be said for it."[3]

The preceding two statements epitomize the enduring struggle that has pitted the law enforcement community against those who are concerned with protecting their privacy interests. The expanded use of advanced technologies in communications has propelled the cryptography debate into the spotlight.

Cryptography uses codes to create secret communication.[4] This system of communication has been used throughout history. One of the earliest known examples of cryptography was used by Julius Caesar when he sent military messages to his armies.[5] Most cryptographic system have two basic functions: encoding and decoding.[6] The encoding function converts the normal data commonly known as "plaintext" into incomprehensible data commonly known as "ciphertext."[7] The decoding function reverses the process, by changing the "ciphertext" back into "plaintext."[8] In order to perform these functions, a sequence of bits, or "keys" must be obtained by the sender and receiver of each message.[9] The strength of the coded communication is greatly dependent upon the length of the key.[10] This system is an

---

1 The term "crypto-genie" was apparently first used by author Steven Levy in 1994. Philip Elmer-Dwitt, *Who Should Keep the Keys?*, TIME, Mar. 14, 1994, at 91.

2 Judy Fahys, *Cryptic Coding: Export Quarrel Touches Utah Coding: Conflict About Sales and Spies*, SALT LAKE TRIB., Jan. 28, 1996, at F2 (quoting James Cavanaugh, NSA's deputy director of public policy).

3 Yale Broad. Co. v. FCC, 478 F.2d 594, 606 (1973) (quoting Lord Devlin).

4 Cryptography is defined as "the science or study of the techniques of secret writing; especially coded cipher systems, methods and the like." RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 485 (2nd ed. 1987).

5 The "Caesar Cipher" adds a number to the position of each letter to the alphabet. If you were to add three to A, the first letter, it would then become D, the fourth letter; C becomes F, and so on. *See* Jeff Prosise, *How To Keep It A Secret; Data Encryption Methods And How They Work*, PC MAG., July 1994, at 315. The Egyptians and Phoenicians were the first known groups of people to utilize cryptography. Edward Radlo, *Legal Issues in Cryptography*, COMPUTER LAWYER, May 1996, at 1.

6 Lance Hoffman, CRYPTOGRAPHY: POLICY AND TECHNOLOGY TRENDS at 4, (visited Jan. 25, 1997) <http://www.eff.org/pub/Privacy/crypto-policy_doe_94.report>.

7 *Id.*

8 *Id.*

9 *Id.* The most common form of key generation in asymmetric cryptography is for an individual to choose two secret 100-digit prime numbers and multiply them together. The 200 digit product reveals the individuals "public key." The private key, the original prime numbers, remain unknown and cannot be determined by the knowledge of the public key. The strength of the keys comes from the fact it is "computationally infeasible" for a modern top-speed supercomputer to determine the factors of a 200-digit number in anything less than several centuries. *See* James Fallows, *Open Secrets*, ATLANTIC, June 1994, at 48. An example of the use of asymmetric cryptography will be discussed in Part I. For a more in-depth discussion of key generation with respect to the different forms of cryptography, see the following publications. *See* Mitchell Moore, *The Role of Cryptography in Network Security*, BUS. COMM. REV., Sept. 1995, at 67; Dave Trowbridge, *Public-key Crypto Gives Privacy Power to the People*, COMPUTER TECH. REV., Apr. 1995, at 7.

10 Hoffman, *supra* note 6. As a recent paper on cryptography asserts that "[t]he sizes of encryption keys are measured in bits and the difficulty of trying all possible keys grows exponentially with the number of bits used. Adding one bit to the key doubles the number of possible keys; adding ten increases it by a factor of more than a thousand." Matt Blaze, *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security* (visited Oct. 12, 1996) <http://www.cdt.org/crypto/>. Therefore, in the case of DES, a 56 bit key, over 72 quadrillion (72,057,594,037,927,936) different possible keys exist. Michael Froomkin, *The Metaphor is the*

example of symmetric or conventional key cryptography. In order for this system to function properly, both the sender and receiver must know the key.

Even though cryptography has been present since the time of Caesar, it has been effectively kept from the American public by the National Security Agency (NSA).[11] Officially, the agency was charged with the duties of monitoring and decoding any signal transmission relevant to national security.[12] Soon after its existence, NSA took substantial steps to control the growth of cryptography.[13] In fact, NSA went so far as to say that it had the "sole authority to fund research in cryptography."[14] For the most part, the claim, has proved to be true, although it lacks legal validity. That is, up until now. With the advancement and growth of the Internet, NSA's claim of sole authority has become somewhat overshadowed.

In the mid 1960's, the Department of Defense's Advanced Research Projects Agency (ARPA) began experimenting with the idea of establishing a computer network to be used for the furtherance of academic research.[15] The concept became reality in 1969, when computers at the University of California of Los Angeles and SRI International in Menlo Park, California were linked and the ARPANET was established.[16] In 1984, ARPANET split into two networks, one of which is now known as the Internet.[17] As of 1996, there were an estimated 30 million users of the Internet worldwide. [18] The impact of this figure is more significant when one realizes the fact that the Internet is growing at a rate of approximately ten percent per month.[19] Because of the growing reliance on the Internet for business transactions and personal communications, the need for a debate on the open architecture and privacy of the network has become tantamount.

Currently, a U.S. citizen or U.S. corporation may domestically use any form or strength of encryption it chooses.[20] The knowledge of encryp-

Key: Cryptography, the Clipper Chip, and the Constitution, 143 U.Pa.L.Rev. 709, 736 (1995). A 128 bit key has over 40 sextillion possible keys. *Id.* at 889.

11 On October 24, 1952, President Truman sent a memorandum to Secretary of State Dean Acheson and Secretary of Defense Robert Lovatt authorizing the existence of NSA and placing it under the authority of the Secretary of Defense. Eleven days later, NSA came into existence. At the time of its creation, there were no press announcements, no news coverage and no Congressional debate. The number of people who work for NSA and the size of its annual budget was and continues to remain classified. Therefore, the agency was often referred to as the "No Such Agency." *A Clipper Primer*, COMPUTER FRAUD & SECURITY BULL., May 1994, at 13; *see also* Maureen Harrington, *Cyber Rebel*, DENVER POST, Mar. 5, 1996, at 24. This publication, without listing its authority, reported that NSA spends one million dollars an hour and eight billion dollars a year on eavesdropping around the world. *Id.*

12 John Perry Barlow, *Decrypting the Puzzle Palace*, COMM. OF THE ACM, July 1992, at 25. The current deputy director of NSA, William Crowell, has stated in a declaration that the two missions of NSA are: (1) to conduct the signals intelligence (SIGINT) activities of the United States Government; and (2) to carry out the responsibilities of the Secretary of Defense concerning the security of the United States national security information systems. *See* Declaration of William Crowell at 2, Karn v. United States Dep't of State, 925 F. Supp 1, (D.C. Cir. 1996) (No. 95-1812). One former Army intelligence officer stated that "SIGINT is more valuable than dope because it goes directly to the personal power and prestige of the President." David Stipp, *Techno-Hero or Public Enemy*, FORTUNE, Nov. 11, 1996, at 180.

13 NSA has attempted to control the growth of private cryptography by relying on the Computer Security Act, which allows for military intelligence agencies' control of the civilian cryptography market. *See* Henry King, *Big Brother, The Holding Company: A Review of Key-Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224, 248-49 (1995). The Computer Security Act of 1987 can be found at Pub.L.No. 100-235, 101 Stat. 1724. NSA has also been instrumental in the development of civilian cryptography and has also attempted to establish universal cryptography standards. *See* Renae Angeroth Franks, *The National Security Agency and Its Interference with Private Sector Computer Security*, 72 IOWA L.REV. 1015 (1987). NSA has also "dispatched FBI agents on break-in missions to snatch code books from foreign facilities in the United States and CIA agents to recruit foreign communications clerks to buy their code secrets." Scott Shane, *Rigging the Game*, BALTIMORE SUN, Dec. 10, 1995, at 8A.

14 David Burnham, THE RISE OF THE COMPUTER STATE 39 (Random House, 1983). In 1975, NSA tried to stop all disbursing of National Science Foundation grants for cryptography research. Kenneth J. Pierce, *Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation*, 17 CORNELL INT'L L.J. 197, 203 (1984).

15 Marie A. Wright, *Protecting Information from Internet Threats*, COMPUTER FRAUD & SECURITY BULL., Mar. 1995, at 7; *see also* Cheryl Ajluni, *Security Techniques Ensure Privacy*, ELECT. DESIGN, Apr. 17, 1995, at 83.

16 Wright, *supra* note 15.

17 Deborah Russel, COMPUTER SECURITY BASICS 211 (1991).

18 Larry Lange, *Net Battleground Awaits Microsoft Salvo*, ELECTRONIC ENGINEERING TIMES, Jan. 8, 1996, at 22.

19 Edward Baig, *Ready to Cruise the Internet?*, BUS. WK., Mar. 28, 1994, at 180.

20 However, this use is restricted primarily to domestic use. The one exception to non-domestic use is contained in a recent amendment to 22 C.F.R. § 123 (1996). The limited exception allows for temporary export for personal use, but also establishes that the when the product is not in possession of the exporter that it should be "lock[ed] . . . in a hotel room safe." 22 C.F.R. § 123.27(a)(3)(ii)(A) (1996). The exporter must also provide a "record of that temporary export and subsequent import." *Id.* at (b).

tion technology may also be distributed domestically to other U.S. citizens without restriction. However, if one chooses to export this technology then he or she faces serious criminal penalties.[21] In the past, a key length of fifty bits is the maximum one is able to export without a license from the Department of State.[22] On January 1, 1997, however, this limit will be raised to a maximum of fifty-six bits as long as the exporting company commits "to explicit benchmarks and milestones for developing and incorporating key recovery features into their products and services."[23] At the end of a two-year period, only those companies that have established a key recovery system and have provided a copy of the keys to a trusted third party will be permitted to export fifty-six-bit key cryptography. [24] Companies and individuals that do not participate in the "key recovery" system will not be permitted to export their cryptographic products.[25] Violation of these restrictions is a criminal offense, punishable by imprisonment.[26]

The argument advanced by the government and law enforcement officials is that strong encryption export regulations are necessary in order for law enforcement authorities to adequately accomplish their job. Recently, FBI Director Louis Freeh testified to a Congressional committee that "encryption capabilities available to criminals and terrorists endanger future usefulness of court-ordered wiretaps."[27] The proposed law enforcement solution comes in the form of "socially responsible encryption products . . . which permit timely law enforcement and national security access and decryption."[28]

The line that separates law enforcement from private individuals and corporations is clearly defined. Law enforcement is concerned with losing its ability to effectively and timely conduct eavesdropping; while individuals are concerned with privacy, freedom of speech and the potential lost revenues. The line between those two is the First Amendment. The First Amendment, which states that no law shall be made that abridges the freedom of speech or of the press,[29] holds the "keys" to resolving this debate.

This paper discusses the government's legitimate concern for national security which has been exhibited through its past attempts and continues through its future intentions of regulating the export of cryptography and addresses the constitutional problems posed by these concerns. Recognizing this dilemma, this paper presents a viable solution that meets the needs of all interested parties without compromising a majority of their ideals and objectives. Part I provides a brief overview of the modern development and explanation of the process of encryption. Part II discusses the regulations and policies that govern the government's efforts in controlling the growth of encryption software through export regulations. Part III discusses the interests and policies of individuals and the business community in the encryption debate. Part IV examines the three encryption cases that have challenged the government's export regulations on First Amendment grounds. Part V presents a First Amendment analysis of encryption source code as speech. Finally, in Part VI, this note presents a possible solution for dealing with the crypto-genie, while at the same time, meeting the needs of the law enforcement, individuals, corporations

---

21 The violation of the Arms Export Control Act (AECA) or the International Traffic in Arms Regulation (ITAR) is punishable by a fine up to $1,000,000, or imprisonment of up to ten years, or both. *See* 22 U.S.C. § 2778(c) (1994); 22 C.F.R. § 127.3 (1996). Any person that knowingly violates the Export Administration Act (EAA) or the regulations of, is subject to a fine of up to five times the value of the exports involved or $50,000 whichever is greater, or imprisonment of up to five years or both. 50 U.S.C. § 2410(a) (1994). Any person that willfully violates the EAA or the regulations of, is subject to five times the value of the exports up to $1,000,000 ($250,000 for an individual), or up to ten years of imprisonment, or both. 50 U.S.C. § 2410(b)(1)(A)(B). The application of these regulations will be discussed in some detail in the text.

22 *See* 57 Fed. Reg. 32,148 (1992); *see also* Dorothy Denning, *Decoding Encryption Policy*, SECURITY MGMT., Feb. 1996, at 59. Note that Executive Order 13026 gives jurisdiction to the Commerce Department. Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996).

23 Statement of the Vice President, Al Gore, CONGRESSIONAL PRESS RELEASE, Oct. 1, 1996. A key recovery system would allow "a trusted [third] party to recover the user's confidentiality key for the user or for law enforcement officials acting under proper authority."

24 Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996).

25 *Id.*

26 *See supra* note 21.

27 Wayne Madsen, *Securing Access and Privacy on the Internet*, COMPUTER FRAUD & SECURITY BULL., Jan. 1, 1996, at 12. The Director made the statement on May 3, 1995 to the House Judiciary Committee.

28 *Impact of Encryption on Law Enforcement and Public Safety*, Hearings on S. 1587 Before the Comm. on Commerce, Science and Transportation, 104th Cong. (1996) (statement of Louis Freeh, Director of Federal Bureau of Investigation).

29 U.S. CONST. amend. I.

and most importantly the First Amendment of the Constitution.

I. THE CRYPTO-GENIE AWAKENS

As previously discussed, symmetric encryption has been around since the time of Caesar.[30] This system provides a means to communicate in secret, but it also creates several problems. One of these problems is key management. To best explain the obstacles that are experienced by using this system, the next section will provide an example involving two fictitious individuals who wish to communicate by using encryption techniques.[31]

Sam (the sender) wishes to send his friend Ruth (the receiver) a personal message. Sam types his message into the computer as plaintext and then uses a previously agreed upon key to encode the message into ciphertext. Sam then sends the message to Ruth. Once Ruth receives the message in ciphertext form, she uses the previously agreed upon key to decode the message into plaintext. At this point, Ruth is able to read her personal message.

One traditional problem that exists with this system is the uncertainty as to whether the sender is actually the person he says he is. Applied to this specific example, how does Ruth in fact know the message is from Sam and not from someone acting as Sam? Once the key becomes known to any other party, the entire security of any message utilizing the key will be compromised.[32] The other problem this system poses is key management. If this was the first communication between the two parties, how does Sam tell Ruth what the key is without compromising the security of future messages? Even if Sam is successful, by telling her in person, the problem still exists if he wishes to change the key in the future or if by chance he wishes to communicate with another party besides Ruth.[33] These key problems of the symmetric system, together with NSA's domination of the development of encryption technologies, created an environment where the use of encryption was underutilized.

In 1975, Whitfield Diffie made a historic discovery that forever changed how encryption is viewed. Whitfield, a computer scientist and cryptographer, has always been "concerned about individuals, an individual's privacy as opposed to Government secrecy."[34] Diffie's discovery made was necessitated by his realization that a perfect system would eliminate the need for a trusted third party.[35] Diffie developed a way to secure the message using two mathematical keys by splitting up the cryptographic key. The system known as public key cryptography or asymmetric cryptography utilizes a public key and a private key.[36] Each party, has a private key which only the owner knows and a public key which everyone knows. Whatever is scrambled by one key, can be unscrambled by the other key. For an explanation on how this system functions, we will revisit Sam and Ruth.

Sam completes a message to Ruth in plaintext form. Upon completion, Sam encodes the message with Ruth's public key. When Ruth receives the message in ciphertext from Sam, she uses her private key to decode the message into plaintext. To send a message back to Sam, Ruth encodes her message with the use of Sam's public key. Sam then uses his private key to decode the message. The knowledge of one half of a key does not in any way compromise the identity of the other half.[37] Therefore, the problem of key management is resolved, eliminating the need for the trusted third party.

The problem of key identification was also elim-

---

30 Edward Radlo, *supra* note 5, at 1.

31 Variations of this example have been used to explain the inner-workings of cryptography. *See* Froomkin, *supra* note 10, at 890-91.

32 This problem is known as key identity or authentication. One method that has dealt with this problem in the past is by distributing the keys by physically secure means. An example would be a bonded courier. This example illustrates the geographic problems that exist with the use of a worldwide network. *See* Moore, *supra* note 9, at 71.

33 With this system of encryption Sam is limited in his freedom to change his keys with Ruth or developing a system with future parties. In either the case of a key that has been compromised with an existing party or the establishment of a key with a new party, Sam has no secure means of communicating the key, other than personally contacting the party.

34 Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES, June 12, 1994, at 47.

35 *Id.* The "trusted third party" that Whitfield Diffie referred to was an individual or service utilized in symmetric encryption systems whom provided key management to senders and receivers by providing them with the keys. In the earlier example of Sam and Ruth, a trusted third party would provide Ruth with a secure key to decode messages from Sam. Whitfield Diffie was concerned that if the trusted third party was served with a subpoena they would simply "sell you out." *Id.*

36 *Id.* at 47-48.

37 *See* Hoffman, *supra* note 6.

inated by the asymmetrical process.[38] The process of authentication or digital signatures could be achieved by reversing the process of encoding. Once again, Sam and Ruth will serve as an example of how the process of authentication works.

In the previous message, Sam encodes a part of the message he wishes to serve as authentication of his identity with the use of his private key. He then encodes the rest of the message with Ruth's public key. Upon receiving the message, Ruth begins by decoding the message using her private key to decode the entire message. She then uses Sam's public key to decode the section of the message in order to prove the authentication of Sam as the sender. At no time throughout this process have either of the private keys been compromised.

In 1977, three inventors Ronald Rivest, Adi Shamir and Leonard Adleman (known as R.S.A.) developed a system which utilized Whitfield Diffie's process of encryption.[39] The R.S.A. system is based on prime number generation, since it is computationally much more difficult to factor two large prime numbers than multiplying them.[40] Some of the companies that utilize RSA technology include: Apple, AT&T, DEC, IBM, Lotus, Microsoft, Northern Telecom and Novell.[41] As of January 1994, over two million instantiations of RSA have been distributed in the United States, and that number is expected to double by the end of 1995.[42]

The use of public key cryptography was relatively unknown to a vast majority of the public until Phil Zimmerman appeared in 1991. The Senate was proposing an anti-crime bill that included a provision that would require manufacturers to insert "trap doors"[43] in their products to enable the government to read encrypted messages.[44] Phil Zimmerman, an information privacy advocate, had recently created an encryption program called Pretty Good Privacy (PGP) that was, and still is, considered a significant obstacle to law enforcement code-cracking efforts. [45] The program uses several encryption methods, including RSA, and uses 512-bit, 1,024-bit, 1,280-bit or 2,048-bit keys.[46] In a recent study, it was concluded that if 100 million personal computers with an operating system of 100 Mhz with eight megabytes of RAM, were devoted to decrypting a PGP-encrypted message using the 1,024-bit key it would take 280,000 years to crack the code.[47] Originally, Zimmerman intended to market his product, but due to a growing concern of possible government intervention that might eliminate any market for his new product, he changed his plans. Zimmerman quickly gave a number of free copies to his friends.[48] "The important thing, reasoned Zimmerman, "was to get PGP out there while it was still legal for people to get a copy — to inoculate the body politic."[49]

Upon receiving PGP, one of Zimmerman's friends commenced driving around for two hours with a laptop and a modem and uploaded PGP from public phones to bulletin boards with In-

---

38 Asymmetric is defined as "not identical on both sides of a central line, unsymmetrical; lacking symmetry." RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE at 129 (2nd ed. 1987).

39 Anthony Watts, *Cryptography is Key to Securing Proprietary Information*, EDN, July 6, 1995, at 101.

40 *See Id.* The author provides an example of the mathematical equation. First, you select two very large prime numbers, P& Q and another number d which is relatively prime to (P-1) * (Q-1). Second you calculate e from the equation e*d'=1 [mod ((P-1) * (Q-1))]. The pair of numbers (e, N) where N is congruent to P*Q is the encryption key; the pair of numbers (d, N) is the decryption key.

41 Susan Landau, *Crypto Policy Perspectives*, COMM. OF THE ACM, Aug. 1994, at 116.

42 Hoffman, *supra* note 6.

43 Traps doors have a weakness in the key part of the encryption algorithm which allows for the holder of such information to use "computational shortcuts to break the code." Froomkin, *supra* note 10, at 736-37. One example is allowing for the holder of the information to simply multiply large prime numbers together verses factoring a large number who can only be factored by two numbers. *Id.* at n.112.

44 Stanley Holmes, *Pretty Good Predicament*, PC WK., July 3, 1995, at A3.

45 John Markoff, *Federal Inquiry on Software Examines Privacy Programs*, N.Y. TIMES, Sept. 21, 1993, D3. The use of encryption by a pedophile hampered the efforts of law enforcement in a recent case in California. *See* Timothy Lennon, *The Fourth Amendment's Prohibition on Encryption Limitation: Will 1995 be Like 1984?*, 83 GEO. L.J. 1849, 1852 n.6 (1995). However, it is unclear whether NSA is unable to crack PGP because of the secrecy that surrounds NSA.

46 Al Berg, *Securing E-mail with Encryption*, LAN TIMES, Sept. 25, 1995, at 142; Douglas Marden, *The Three Cs to Improving UNIX System Security*, ENT. SYS. J., Mar. 1995, at 90.

47 Trowbridge, *supra* note 9, at 10.

48 Homes, *supra* note 44.

49 *Id.* Zimmerman and other civil libertarians are quick to point out that PGP has been utilized on at least two occasions against oppressive governments. The first occasion occurred when Burmese freedom fighters used PGP to keep documents hidden from their government. The second occasion took place when Zimmerman received a message from an individual in Latvia that stated, "Let it never be, but if dictatorship takes over Russia, your PGP is widespread from Baltic to Far East now and will help democratic people if necessary." *See* Levy, *supra* note 34, at 50.

ternet connections.[50] The fact that the encryption program was now on the Internet meant that it was readily accessible to foreigners or exportable without a license.[51] What occurred next was a fifteen month investigation led by the Department of Justice in order to determine if Zimmerman should be indicted on federal charges.[52] As a result of the Zimmerman affair, the government's policy on Internet distribution remained unclear. A statement by an assistant attorney general that there is "no change in the law, no change in policy. If you're planning on making encryption available over the Internet, or other means, better check with the State Department first," did nothing but cloud the issue further.[53]

Zimmerman, undaunted by the government's efforts, recently developed a program entitled PGPphone, which uses the Blowfish algorithm. [54] With the development of the technology to make voice phone calls over the modem, this program encodes or rearranges the digital version of the phone conversation and then decodes it on the other end.[55] This program, has been available on the Internet for downloading and at publication, [56] there have been no announcements that the Department of Justice is investigating the matter.[57]

II. THE GOVERNMENT'S (POROUS) AIR TIGHT BOTTLE

Up until October 1, 1996, cryptographic systems and equipment were considered a munition.[58] As a munition, cryptography was subject to the Arms Control Export Act (ACEA) which gives the President the authority to designate certain items as defense articles or defense services.[59] The export of these designated items is controlled by regulations under the International Traffic in Arms Regulations (ITAR).[60] The United States Munitions List then forms the index of the items designated as "defense articles."[61] Defense services are defined as the "furnishing of assistance (including training) to foreign persons, whether in the United States or abroad. . ."[62] and the "furnishing to foreign persons of any technical data controlled under this subchapter, whether in the U.S. or abroad."[63] Encryption software was classified as technical data because of its capability of maintaining secrecy,[64] and also for its ability con-

50 Andrew Brown, *Kings of the Wired Frontier*, THE INDEPENDENT, Apr. 30, 1995, at 16. Zimmerman has repeatedly denied that he placed his program on the Internet.

51 The program is readily available outside the United States without the approval of the U.S. Government. A Norwegian web site, (visited Jan. 25, 1997) <http://www.ifi.uio.no/pgp/download.shtml>, lists several alternate web pages in other countries where the program may be downloaded. The countries include: Australia, Austria, Germany, Italy, Japan, Mexico, Switzerland and the United Kingdom. A Finnish web site boasts to provide the "PGP source code and binaries" to any user without any approval necessary. *See* Second Declaration of Julia Kogan, In Support of Plaintiff's Reply to Defendants' Opposition to the Motion for Preliminary Injunction, Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996).

52 The result of the investigation was announced on, January 11, 1995, where the Department of Justice summarily announced that "the investigation has been closed," without any further comment. (visited Jan. 25, 1997) <http://www.eff.org/pub/Alerts/usatty_pgp_960119.announce>.

53 *Government Drops Zimmerman PGP Prosecution*, NEWSBYTES NEWS NETWORK, Jan. 12, 1996, at 2.

54 *Product Bits: Zimmerman Goes for Phone Privacy Software*, TELECOMWORLDWIRE, Jan. 17, 1996, at 1.

55 *Id.* The use of this technology allows the callers to totally bypass the long distance network. Some companies that offer the service known as Internet Phone include: VocalTec, Camelot, Quarterdeck and ITEL. For a further explanation of this issue and a recent FCC petition which requests the service to be discontinued; *see ACTA's Petition for Declaratory Ruling, Special Relief and Institution of Rulemaking*, RM-8775 (Mar. 4, 1996).

56 *See* Wendy Grossman, *Innovations: Secretly Does It*, DAILY TELEGRAPH, Apr. 2, 1996, at 26 (for further explanation of PGPphone).

57 At publication, there were no announced Department of Justice investigations. This information was obtained by a telephone call to the Department of Justice, an Internet search and a Lexis/Nexis search.

58 On this date the Vice President Al Gore announced the administration's intention to remove cryptographic systems from the Munitions List and place them under the jurisdiction of the Commerce Department. The Executive Order signed by the President was signed on November 15, 1996. Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996). A munition is restricted from being exported without a valid license, (e.g., a cruise missle or nerve gas).

59 22 U.S.C. § 2778 (1994).

60 22 C.F.R. § 120 (1996).

61 *Id.* § 121.1.

62 *Id.* § 120.9(a) (1).

63 *Id.* § 120.9(a) (2).

64 The definition of technical data includes "Software as defined in 22 C.F.R. § 121.8(f) of this subchapter directly related to defense articles." *Id.* § 120.10(4). Section 121.8 defines software as "Software includes, but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair." Cryptographic software, as aforementioned is on the USML at 22 C.F.R. § 121.1 (XIII)(b)(1), which states that "cryptographic . . . software with the capability of maintaining secrecy or confidentiality of information or information systems."

cerning defense services.[65]

On November 15, 1996, President Clinton signed Executive Order 13026 which removed cryptographic systems from the Munition's List. [66] The President then placed the jurisdiction of regulating the export of cryptographic systems under the authority of the Commerce Department.[67] Under the Commerce Department's applicable regulations, cryptography would be considered a dual-use commodity under the Export Administration Regulations (EAR).[68] However, the Executive Order specifically states that separate provisions will be established to control "export and foreign dissemination of encryption products."[69] Therefore it is necessary to examine both the ITAR and EAA regulations and procedures in order to determine potential problems that exist, in order to avoid them in the implementation of future regulations.

Under the ITAR, when an applicant wishes to export an article or service and doubt exists as to whether the article or service is listed on the U.S. Munitions List, the applicant must apply to the State Department's Office of Defense Trade Controls (ODTC).[70] The applicant must file a "Commodity Jurisdiction Request" (CJR) to determine if a license is required. [71] If it is determined that a license is required, then the applicant must register with the ODTC. [72] Upon registration approval, the applicant must obtain a license from ODTC and seek advance approval for each recipi-

65 22 C.F.R. § 120.10(2) (1996).

66 Exec. Order 13,026, 61 Fed. Reg. 58,767 (1996).

67 *Id.*

68 The initial determination that cryptography was a dual-use technology was made in 1991 by the Coordinating Committee on Multilateral Export Controls. *See* Susan Landau, *Codes, Keys and Conflicts: Issues in U.S. Crypto Policy* chap. 8 (visited Jan. 25, 1996) <http://info.acm.org/REPORTS/ACM_CRYPTO_STUDY/_WEB/contents.html>. Dual-use is defined as "items that have both commercial and military or proliferation applications." 15 C.F.R. § 772 (1996). In fact, the Department of Commerce does already regulate cryptographic systems containing functions "generally limited to purposes such as data authentication, password protection, and access control." Draft Memorandum from Bruce W. McConnell and Edward J. Appel, Co-Chairs, Interagency Working Group on Cryptography Policy to All Interested Parties 23 (May 20, 1996). The EAR are administered by the Bureau of Export Administration in the Department of Commerce. The statutory authority for the EAR, the Export Administration Act of 1979, 50 U.S.C. app. § 2401 (1994), lapsed on August 20, 1994. *See* 50 U.S.C. app. § 2419 (1994). President Clinton issued executive orders requiring that the EAR be kept in force to "the extent permitted by law" under the International Emergency Powers Act (IEPA), 50 U.S.C. § 1701 (1994). *See* Exec. Order No. 12924, 59 Fed. Reg. 43,437 (1994); *See* 61 Fed. Reg. 42,527 (1996). The EAR was subsequently greatly revised and simplified. *See* 61 Fed. Reg. 12,714 (1996).

69 Exec. Order 13,026, 61 Fed. Reg. 58,767 (1996). The Executive Order states that the foreign availability exception shall not apply, the Department of Justice shall be a voting member on the Export Administration Review Board and that appropriate controls may be established to "promote . . . the development of a key recovery management infrastructure." *Id.* The establishment of separate procedures to govern the forms of cryptography removed from the Munitions List is consistent with the previous government actions. On October 12, President Clinton transferred commercial communication satellites and hot section technologies for the development, production, and overhaul of commercial aircraft engines from the United States Munitions List to the Commerce Control List. Exec. Order No. Amend. 12,981, 61 Fed. Reg. 54,079 (1996). The separate procedures established by Executive Order included a necessary majority vote from the Operating Committee to determine whether the item is exportable. All other items must only be ruled on solely by the Operating Committee's Chairperson, the Secretary of Commerce. *Id.* This procedure is important to note when one examines the defense oriented membership of the Operating Committee. The Committee is composed of representatives of the Departments of Commerce, State, Defense, Energy, and the Arms Control and Disarmament Agency. Representatives of the Joint Chiefs of Staff and the Nonproliferation Center of the Central Intelligence Agency are also in attendance, but do not vote. Exec. Order No. 12,981, 60 Fed. Reg. 62,981 (1995). Shortly after the Executive Order, the Department of Commerce established its own, separate procedures to govern the export of these two items. Commercial Communication Satellites and Hot Section Technology for Development, Production or Overhaul of Commercial Aircraft Engines, 61 Fed. Reg. 54,540 (1996). These rules amended the EAR to exclude the two items "from the mandatory foreign availability decontrol or export licensing provision of the EAR, and from Special Comprehensive License eligibility." *Id.* Further, each request would be determined on a "case-by-case review" and only granted export privileges if it was "consistent with U.S. national security and foreign policy interests." *Id.* The factors that would be examined by the Operating Committee are: (1) country of destination; (2) ultimate end-users; (3) technology involved; (4) specific nature of the end-use(s); and (5) types of assurance against unauthorized use or diversion that are given in a particular case. *Id.* at 54,541.

70 22 C.F.R. § 120.4(a) (1996).

71 *Id.* The Deputy Director of NSA recently testified that all "[l]icense applications for the permanent or temporary export of cryptographic products are forwarded by the State Department to NSA "for an assessment of whether the approval of an export license could have a negative impact on the national security interests of the United States. In making this assessment, NSA considers several factors including the sensitivity of the technology proposed for export, and the declared end-user and end-use of the commodity. Declaration of William Crowell at 4, Karn v. United States Dep't of State, 925 F. Supp 1, (D.C. Cir. 1996).

72 22 C.F.R. § 120.4(b) (1996). The applicant is required to register as an "arms dealer." Bill Pietrucha, *Judge Hears Arguments To Dismiss Encryption Case*, NEWSBYTES, Sept. 23, 1996, at 4.

ent of the article or service.[73]

In 1978, a Department of Justice memorandum was written to a science advisor of President Carter, reporting on the constitutional concerns of the ITAR regulations.[74] It was asserted that the ITAR prohibitions on cryptographic ideas and information "amounted to an unconstitutional prior restraint." [75] The two fatal flaws that the author cites are "the standards governing the issuance or denial of licenses are not sufficiently precise to guard against arbitrary and inconsistent administrative action; second, there is no mechanism established to provide prompt judicial review of State Department decisions barring disclosure."[76] The author also asserts that the argument that the ITAR regulates conduct not speech,[77] is misplaced because "even a cursory reading of the technical data provisions reveals that those portions of the ITAR are directed at communication." [78]

Interestingly enough, current members of the Justice Department have ignored this point and instead have argued that *O'Brien* does apply.[79] In summary, the memorandum asserted that the requirement of a "prepublication review" of cryptographic information might meet first amendment standards if the "necessary procedural safeguards" were put into existence. [80] This memorandum was affirmed by the Department of Justice as recently as 1984.[81] The 1984 memorandum also warned that ITAR's prohibitions of "communications of unclassified information by a technical lecturer at a university or to the conversation of a United States engineer who meets with foreign friends at home to discuss matters of a theoretical interest," were forms of unconstitutional prior restraint. [82]

Under the EAA, all regulated commodities are placed on the Commerce Control List (CCL).[83] Items or technology is identified by the Secretary of Defense in concurrence with Secretary of Commerce as subject to export controls via the CLL. [84] The CCL indicates whether and to what extent, a commodity is controlled. Controls may be implemented for national security, foreign policy, short supply and other purposes. [85] Concerning national security, there are three possible options available for the Secretary of Commerce to choose from when designating an commodity on the CCL.[86] In regards to foreign policy, there are

---

73 In addition to the requirement of supplying the name of each particular recipient, the applicant must also have the following statement upon the bill of lading and invoice; "[t]hese commodities are authorized by the U.S. Government for export only to [country of ultimate destination] for use by [end-user]. They may not be transferred, transshipped on a non-continuous voyage, or otherwise be disposed of in any other country, either in their original form or after being incorporated into other end-items, without the prior written approval of the U.S. Department of State." 22 C.F.R. § 123.9(b) (1996).

74 Memorandum from John M. Harmon, Assistant Attorney General, Office of Legal Counsel, Department of Justice to Dr. Frank Press, Science Advisor to President Carter (May 11, 1978) (on file with the Department of Justice).

75 *Id.* at 5.

76 *Id.* at 10.

77 If the regulation affected speech, then the application of the *O'Brien* test would be necessary. The *O'Brien* test arises from a Supreme Court case that established a four part test for determining when conduct reaches the level of speech, and as such, is protectable by the First Amendment. O'Brien v. United States, 391 U.S. 367 (1968).

78 Memorandum from John M. Harmon, *supra* note 74 at 11, n.16.

79 The government argued that *O'Brien* applied in both the *Bernstein* and *Karn* cases. Memorandum of Points and Authorities in Support of Defendants' Motion for Summary Judgment at 12-14, Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (C.D.Cal. 1996); Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss, or in the Alternative, for Summary Judgment at 17-20, Karn v. U.S. Dep't of State, 925 F. Supp. 1 (D.C. Cir. 1996).

80 Memorandum from John M. Harmon, *supra* note 74 at 17-18.

81 "We remain of the opinion . . . the ITAR still present some areas of potentially unconstitutional application, and, moreover, that we cannot be certain whether existing case law would be sufficient to narrow the range of application to a constitutionally sufficient extent." Memorandum from Larry L. Simms, Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice to Davis R. Robinson, Legal Advisor, Department of State at 14 (July 5, 1984). A 1981 DOJ memorandum also concluded that the ITAR regulations were an unconstitutional form of prior restraint. Memorandum from Theodore Olson, Assistant Attorney General, Office of Legal Counsel, U.S. Dep't of Justice to William B. Robinson, Office of Munitions Control, U.S. Dep't of State at 202 (July 1, 1981).

82 Memorandum from Larry L. Simms, supra note 81. This statement clearly reflects the issues surrounding *Bernstein*. *Bernstein*, 922 F. Supp. 1426. In this civil action, which will be discussed later in greater depth, the plaintiff is a graduate student (has now since graduated and wishes to teach) in mathematics, wishes to publish a mathematical paper on algorithms. The State Department has denied all of his requests to export his paper. Bernstein is currently suing the government on First Amendment grounds.

83 50 U.S.C.S. § 2404(c)(1) (Law Co-op. 1996).

84 *Id.* at (c)(2). Failure to act by either the Secretary of Defense or President, within 20 days, leads to an affirmation of the Secretary of Commerce's determination concerning the item or technology. *Id.*

85 15 C.F.R. § 799.1(d)(1)(iii) (1996).

86 Validated licenses are required based on national security when:

five options that the President, after consulting Congress,[87] may choose from when imposing export controls under the CCL.[88] An applicant wishing to export a commodity contained on the CCL must apply for a validated license.[89] The application requires extensive documentation[90] and is reviewed on a case-by-case basis.[91] Within sixty days after receipt of the license application, the Secretary of Commerce shall formally issue or deny the license.[92] If a license for application is denied the Secretary must state the statutory basis and the policies that are furthered by the denial.[93]

Unlike the ITAR, the EAA establishes provides an appeal process where license denials may be reviewed by an administrative law judge.[94] However, all determinations made by the administrative law judge are reviewed by the Secretary of Commerce who either affirms or vacates the decision.[95] This ineffective judicial review combined with the fact that all functions exercised under the EAA are explicitly excluded from judicial review and the protections of the Administrative Act,[96] causes ample concern of the possibility of arbitrary and inconsistent administrative action. One provision that could be easily abused in the implementation of export controls of cryptographic systems is the foreign availability exception.[97] This exception allows the President to place export restrictions on goods or technology that are "available without restriction from other sources outside the United States . . . [if] . . . the absence of such controls would prove detrimental to the foreign policy or national security of the United States."[98] The Director of the FBI and a

(1) the export of such goods or technology is restricted pursuant to a multilateral agreement, formal or informal, to which the United States is a party and, under the terms of such multilateral agreement, such export requires the specific approval of the parties to such multilateral agreement; (2) with respect to such goods or technology, other nations do not possess capabilities comparable to those possessed by the United States; or (3) the United States is seeking the agreement of other suppliers to apply comparable controls to such goods or technology and, in the judgment of the Secretary, United States export controls on such goods or technology, by means of such license, are necessary pending the conclusion of such agreement.

50 U.S.C.S. § 2404(e)(2)(A)-(C) (Law Co-op. 1996).

87 50 U.S.C.S. § 2405(f)(1)(2) (Law Co-op. 1996) (stating that the President must consult specifically with the Committee on Foreign Affairs of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate before he may impose, expand or extend export controls).

88 The five options are:

(1) such controls are likely to achieve the intended foreign policy purpose, in light of other factors, including the availability from other countries of the goods or technology proposed for such controls, and that foreign policy purpose cannot be achieved through negotiations or other alternative means; (2) the proposed controls are compatible with the foreign policy objectives of the United States and with overall United States policy toward the country to which exports are to be subject to the proposed controls; (3) the reaction of other countries to the imposition, extension, or expansion of such export controls by the United States is not likely to render the controls ineffective in achieving the intended foreign policy purpose or to be counterproductive to United States foreign policy interests; (4) the effect of the proposed controls on the export performance of the United States, the competitive position of the United States in the international economy, the international reputation of the United States as a supplier of goods and technology, or on the economic well-being of individual United States companies and their employees and communities does not exceed the benefit to United States foreign policy objectives; and (5) the United States has the ability to enforce the proposed controls effectively.

50 U.S.C.S. § 2405(b)(1)(A)-(E) (1996).

89 *Id.* § 2403.

90 15 C.F.R. § 772 (Supp. 1) (1996). Some of the information that must be submitted include the ultimate consignee in the country of ultimate destination, an intermediate consignee in any intermediary in a foreign country who participates as an agent, description for the end-use intended by the ultimate consignee and computer performance as calculated in Composite Theoretical Performance. *Id.*

91 50 U.S.C.S. § 2409(b) (1996).

92 *Id.* § 2409(f)(1).

93 *Id.* § 2409(f)(3)(A)-(C).

94 *Id.* § 2412(e). The ITAR expressly states that designation of items as defense articles or services is not subject to judicial review. 22 U.S.C.S. § 2778(h) (1996).

95 50 U.S.C.S. § 2412(e) (1996). As a result, the so-called "judicial review" appears like simple window dressing. The statute clearly states that the Secretary's decision is "final," leaving little doubt as to the weight of the administrative law judge's determination.

96 50 U.S.C.S. § 2412(a) (Law Co-op. 1996).

97 50 U.S.C.S. § 2403(c) (Law Co-op. 1996). However, as was with the case with other items recently transferred from the United States Munitions List to the Commerce Control List, the foreign availability exception will not be applied to cryptography. This will undoubtedly present an even greater threat to an individual's liberties. The export determination, made by a defense oriented Operating Committee, will be guided solely by the determination of whether it is consistent with U.S. national security and foreign policy interests, regardless of the availability of the item elsewhere.

98 *Id.* One concern shared within the intelligence community is that this exception will demand for their agencies to provide sensitive information in order to refute claims of foreign availability or overriding national security concerns thereby exposing the abilities and objectives of highly classified missions. One example of this would be the case where an applicant wishes to export a 90 bit key program to India. The applicant asserts that India has 90 bit key generally avail-

number of other intelligence officials contend that the President would not be hard pressed to utilize this exception.[99]

Regardless of the preclusion of judicial review, the courts have recognized that "colorable constitutional claims may be reviewed by the courts."[100] Therefore, if licenses were denied on the basis of "impermissible reasons" or in excess of the Secretary's authority, the action would be reviewable by the court.[101] Another legal tool may also exist for cryptographic exporters by relying on a prior decision. Ordinarily, "where a determination made in an administrative proceeding is to play a critical role in the subsequent imposition of a criminal sanction, there must be some meaningful review of the administrative proceeding."[102] However, the 9th Circuit refused to apply this principle in regard to the EAA because the decision to control a commodity "does not involve the defendant's individual rights and is not an element of the criminal offense in the pending case."[103] This analysis applied to export control of cryptographic systems, which involves first amendment rights, most certainly promises a different result.

The classification of goods or technology on the CCL is precluded from review, which if violated, will subject the individual to criminal sanctions. The EAA's functions are explicitly excluded from judicial review and the protections of the Administrative Procedures Act.[104] As shall be asserted later, the limitation of export cryptography is a violation of one's First Amendment rights. Therefore, the lack of a "meaningful review" in the case of controlling the export of cryptographic systems will not pass constitutional muster under existing EAA regulations.

As the new procedures governing the control of export of cryptographic systems are developed it is tantamount for the government to recognize the widespread dissemination of encryption products throughout the world. A study conducted in June of 1996 identified 532 foreign encryption products originating from twenty-eight foreign countries.[105] The Internet, a worldwide accessible system, has over thirty-five cryptographic programs available for download, all of which are over the exportable limit of "40-bit keys."[106] In an attempt to demonstrate the absurdity in the United States export restrictions, a witness, who later testified before Congress, recently downloaded of these programs from a FTP site.[107] The abundance of encryption products is evidenced by the fact that for as little as five dollars, one can buy a "U.S. export restricted" encryption program on the streets of Saint Petersburg, Russia.[108]

A. An Attempt to Plug the Leaks

On November 16, the Clinton Administration, in an attempt to appease the needs of the com-

able in this particular country. The intelligence community would be forced to present evidence that India does or does not have this capability, which may result in the release of highly sensitive intelligence information. Interview with an anonymous intelligence government official, in Washington, D.C. (Oct. 11, 1996) (notes on file with COMMLAW CONSPECTUS).

99 Director Freeh testified to Congress that the use of encryption products "by a vast array of criminals and terrorists to conceal their criminal communications and information poses an extremely serious and, in my view, unacceptable threat to public safety." And without the ability to promptly decrypt encrypted communication the Director stated that "[the Bureau] will not be able to effectively fulfill our mission of protecting the American public." Impact of Encryption on Law Enforcement and Public Safety: Hearings on S. 1587 Before the Comm. on Commerce, Science and Transportation, 104th Cong. (July 25, 1996) (statement of Louis Freeh, Director of Federal Bureau of Investigation) (visited Sept. 30, 1996) (available at <http://www.crypto.com>). The Deputy Director of NSA testified that "if encryption is used by criminals and other adversaries (e.g., terrorism) to help hide their activities, the public safety of U.S. citizens, and citizens of other countries, may be placed in jeopardy." Security and Freedom through Encryption Act: Hearings on H.R. 3011 Before the House Judiciary Comm. 104th Cong. (Sept. 26, 1996) (statement of William Crowell, Deputy Director of NSA).

100 United States v. Bozarov, 974 F.2d 1037, 1044 (9th Cir. 1992), *citing* Webster v. Doe, 486 U.S. 592, 602-05 (1988) (recognizing that if the Secretary abused his authority by denying licenses arbitrarily, judicial review would not be precluded.)

101 *Bozarov*, 974 F.2d at 1044-45.

102 Estep v. United States, 327 U.S. 114, 121-22 (1946).

103 United States v. Mandel, 914 F.2d 1215, 1221 (9th Cir. 1990).

104 50 U.S.C.S. § 2412(a) (Law Co-op. 1996).

105 David Balenson, Representative of Trusted Information Systems Inc., Remarks at the Annual International Cryptography Institute Conference (Oct. 26, 1996) (discussing report issued by the Software Publishers Association).

106 John Black, *The Internet Export Control Gap — The Reality vs. The Reality*, EXPORT CONTROL NEWS, June 30, 1995, at 9.

107 Export Controls on Mass Market Software: Hearing Before the House Foreign Affairs Subcommittee on Economic Policy, Trade and Environment, 103rd Cong., 1st Sess. 5-9 (1993) (statement of Ray Ozzie, President Iris Associates).

108 Barlow, *supra* note 12, at 27.

puter industry, "unilaterally"[109] proposed a new initiative to replace previous Clipper proposals.[110] The initiative, Clipper III, specifies that for the next two years, industry will be permitted to export encryption products of up to fifty-six-bit key, provided the industry makes a commitment to work towards "developing and incorporating key recovery features into their products and services."[111] The key recovery features allow for a trusted third party to recover the user confidential key for the user or law enforcement with the proper authorization.[112] At the end of the two year time period, with a completion of a key recovery infrastructure,[113] export of fifty-six-bit key products not supporting the key recovery system will not be permitted.[114]

After the Clipper III proposal was announced, eleven companies formed an alliance to develop a "worldwide approach to strong encryption" that would utilize a key recovery system.[115] Although the alliance was quick to form, it does not appear as if all the members of the alliance fully support the proposal. In fact, the chief executive of RSA Data Security Inc., called the government's announcement "disastrous."[116] The manufacturer of the most popular Internet browser, Netscape Communications Corp., also warned that the plan "would hinder the industry's ability to compete internationally."[117] The Business Software Alliance also pointed out that several issues have yet to be resolved, including the definition of key recovery system.[118]

The carrot and stick approach taken by the government is seen by some industry officials as "extortion."[119] For the companies that abide by the government's wishes of developing a key recovery infrastructure, they will be allowed to export at their convenience; whereas companies that do not take part in the development of a key recovery system will be prohibited for exporting their encryption products.[120] Individuals who wish to export encryption software, are completely ignored by the government's proposal. Under the proposal, at the end of the two year period, a student or

109 Both Senator Leahy and Senator Burns expressed displeasure with the fact that the administration had not consulted with Congress before announcing the new initiative. *See Statement by Senator Leahy on Administration's Encryption Initiative*, U.S. NEWSWIRE, Oct. 2, 1996, at N1; *Burns Cautious on Encryption Plan*, CONGRESSIONAL PRESS RELEASES, Oct. 1, 1996.

110 The initiative has been touted as "new" by the administration, but one House Commerce Committee staff member stated that the initiative was "key escrow warmed over, and that's it." *White House to Revive "Clipper" Wiretap Plan*, BUS. WIRE, May 18, 1996. The original Clipper proposal was a NSA-developed, hardware-oriented, cryptographic device that utilizes a symmetric encryption and decryption algorithm called "Skipjack." Dorothy Denning, *Clipper Chip will Reinforce Privacy*, WASH. TIMES, Oct. 24, 1994, at 20. The Skipjack algorithm remains classified, "to protect the security of the key escrow system," but the length of the key has been stated at 64 bits software / 80 bits hardware. *Statement by Press Secretary for the White House*, Apr. 16, 1993 (visited Jan. 25, 1997) <http://www.eff.org/pub/Privacy/wh_crypto_original.announce>. All phones and modems equipped with the "voluntary" Clipper Chip would provide secure encryption, but with a built-in decryption capability, that allows authorized officials, with the cooperation of two other parties, to decode the data. Dorothy Denning, *The Case for the Clipper*, TECH. REV., July 1995, at 50. With the proper court authorization, law enforcement agencies could obtain the keys from the escrow agents and then would be able to decrypt the message. In April of 1994, the government received a scare concerning the security of the Clipper chip. The arrest of double agent Aldrich Ames allegedly prompted a meeting involving the CIA, FBI and NSA where it addressed the possibility that information concerning the Clipper had been sold to the Russians. *Spy Scandal Could Sink Clipper*, DATA COMM., Apr. 1994, at 17. (information provided by Winn Scwartel, an executive director of a security consultancy, who had spoken with an individual who had attended the meeting). The anonymous source was quoted as saying that if the Clipper had been compromised then "the whole thing's over, and we have to start from scratch." *Id.* Government officials that were questioned about the meeting, neither confirmed nor denied its existence. *Id.*

111 Statement of the Vice President, Al Gore, CONG. PRESS RELEASE, Oct. 1, 1996.

112 *Id.* The data recovery feature of the key recovery system for the specific user is unnecessary and superfluous based on the fact that "data recovery can be done independently . . . and in a more secure manner." Center for Democracy and Technology, *Preliminary Analysis of "Clipper III" Encryption Proposal* (visited Jan. 25, 1997) <http://www.cdt.org/crypto/clipper_III/clipper_III_analysis.html>.

113 It is unclear what will occur if industry is unable to meet the fanciful demand of establishing a key recovery infrastructure in a two year time period.

114 Statement of the Vice President, Al Gore, CONG. PRESS RELEASE, Oct. 1, 1996.

115 *Joint Press Announcement: High Tech Leaders Join Forces to Enable International Strong Encryption*, BUS. WIRE, Oct. 2, 1996. The eleven companies are: Apple Computer, Inc., Atalla, Digital Equipment Corporation, Groupe Bull, Hewlett-Packard Company, IBM, NCR Corp., RSA, Sun Microsystems, Inc., Trusted Information Systems and UPS.

116 John Markoff, *IBM's Rivals Criticize U.S. Encryption Compromise*, INT'L. HERALD TRIB., Oct. 3, 1996, at 14.

117 *Id.* U.S. industry's concern stem from the fact that competitor countries are not restricted by export regulations and therefore are more attractive to consumers who value unlimited security. Fahys, *supra* note 2, at F1.

118 *Encryption and Indecency; Administration Acts on 2 On-Line Fronts*, COMMUNICATIONS DAILY, Oct. 2, 1996, at 2.

119 Markoff, *supra* note 116.

120 Companies that do not take part in the key recovery system will still be permitted to export encryption products that are 40 bit keys and under.

teacher of encryption would be prohibited from placing their encryption software or code upon the Internet without first taking part in the government-mandated key recovery system.

Another concern that arises from the Clipper III proposal is the issue of implementation on a worldwide scale. Quite simply, why would a foreign government and foreign companies wish to take part in a program that allows the U.S. to eavesdrop when it is just as easy to buy more powerful encryption software that prevents such an intrusion? Administration officials respond by asserting that foreign governments that want access to U.S. encryption keys will apply to U.S. courts, and when the U.S. government needs a foreign country's encryption keys the reciprocal shall apply.[121] However, this answer only presents more questions. What about countries that do not participate? What about countries who have less protective laws than the U.S.? What about countries that violate the procedures in the name of national security?

Another issue that is presented by the government's proposal is the ability of criminals to simply encrypt on top of a legal encryption communication. This issue was raised throughout the earlier Clipper proposals and the government's stock answer has been and most likely will continue to be, "criminals need to communicate with others nationally and internationally, including not just criminal confederates but also legitimate organizations such as banks."[122] However, this same official later listed several examples of how "harmful" encryption was being utilized by criminals.[123] In not one of the examples, was the criminal communicating with a "legitimate organization." Another instance also serves as an example of the misguided policy statements of the government. At a recent Congressional hearing where the Deputy Director of NSA was asked about the widespread availability of encryption products on the Internet, he flatly contended that "serious users of security products don't obtain them from the Internet."[124] But only minutes later, the Deputy Director discussed the extreme dangers of PGP, an encryption program readily available on the Internet, to the effectiveness of the law enforcement.[125] From these two examples, it is apparent that the government's main concern is the development of a single government accessible encryption standard.

B. Without the Clipper, "the government will eventually become helpless to defend the nation from terrorism and other threats"[126]

The authority to conduct electronic surveillance, or wire tap, originated from the 1968 Omnibus Crime Control and Safe Streets Act.[127] Between 1978 and 1988, there were a total of 7,200 applications for electronic surveillance, of which only 11 were denied.[128] In 1993, not a single wiretap request was denied.[129] In 1994, the FBI and NSA requested 576 warrants to eavesdrop on foreigners within the United States, none of which were denied.[130] The FBI has stated that wiretap

121 *See Encryption and Indecency; Administration Acts on 2 On-Line Fronts, supra* note 118.

122 *See Impact of Encryption on Law Enforcement and Public Safety, supra* note 28. However, this argument is less convincing when applied to terrorists who survive in large part from isolating and hiding from all legal aspects of society.

123 The examples listed by the Director of the FBI were: (1) In the Aldrich Ames spy case, where Ames was told by his Soviet handlers to encrypt computer file information to them; (2) In a child pornography case, where one of the subjects used encryption in transmitting obscene and pornographic images of children over the Internet; (3) In a major drug-trafficking case, where one of the subjects of one of the court-ordered wiretaps used a telephone encryption device which frustrated the surveillance; (4) Some of the anti-Government Militia groups are now advocating the use of encryption as a means of preventing law enforcement from properly investigating them.
Impact of Encryption on Law Enforcement and Public Safety, supra note 28.

124 *Security and Freedom through Encryption Act: Hearings on H.R. 3011 Before the House Judiciary Comm.* 104th Cong. (Sept. 26, 1996) (statement of William Crowell, Deputy Director of the National Security Agency.

125 *Id.*

126 James Aley, *How Not to Help High Tech*, FORTUNE, May 16, 1994, at 100 (statement by Louis Freeh, Director of Federal Bureau of Investigation).

127 Electronic Communications Privacy Act of 1986, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 211-25, *reprinted in* 1968 U.S.C.C.A.N. 237, 253 (codified at 18 U.S.C. § 2510 (1994).

128 Denning, *supra* note 110. However, this might be attributed to the higher requirments required of law enforcement in applying for a wiretap.

129 Robin Hanson, *Can Wiretaps Remain Cost Effective?*, COMM. OF THE ACM, Dec. 1994, at 15.

130 Scott Shane, *National Security Agency: Catching Americans in NSA's Net*, BALTIMORE SUN, Dec. 12, 1995, at 15A. In this type of instance the intelligence agency must gain approval from the Foreign Intelligence Surveillance Court, which is solely composed of seven federal judges, appointed to seven-year terms by the chief justice of the United States Supreme Court. Of the 576 requests, all were granted by the court. *Id.* Clearly when a message is encrypted above the

surveillance from 1985 to 1991, has led to 7,324 convictions.[131] This last figure must be given limited value because it only serves as a rough estimate, since it assumes that these convictions would have been impossible without the wiretaps. The average cost of conducting a wiretap, as of 1993 was $57,256.[132] According to a recent FBI study, the costs will soon increase seventeen times[133] due to advances in technology, such as fiber-optic cable and advanced call forwarding.[134] As criminals and terrorists develop more sophisticated illegal activities, through the use of advanced technologies, the continued effectiveness of law enforcement's efforts to eavesdrop becomes critical.

With the expansion of the Internet, the government has sought to protect their law enforcement abilities by advancing particular cryptography standards and influencing the debate.[135] One initiative advanced by the government, the Clipper, has continually been asserted as "voluntary." However, in a recently declassified secret FBI document entitled "Impact of Emerging Telecommunications Technologies on Law Enforcement," it was stated that a necessary goal was to "prohibit cryptography that cannot meet the Government standard. An exception will, of course, exist for the protection of classified, national defense information."[136]

Another recent declassified document prepared by the FBI, NSA and DOJ stated that "[t]echnical solutions, such as they are, will only work if they are incorporated into *all* encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required."[137] These memoranda have substantial support in a number of the actions taken by the government. It is no secret that the United States government has an enormous market power that could be used to influence the development or implementation of products.[138] For example, shortly before the introduction of the Clipper I initiative, AT&T had developed a new, low cost secure phone that was designed with a nonexportable encryption algorithm.[139] After some consultations with NSA, AT&T refitted their phones with the Clipper chip. Immediately thereafter, the Justice Department placed an eight-million dollar order with AT&T for Clipper-based encoding devices.[140] The Defense Department is also believed to have ordered 20,000 chips.[141] Just this year, AT&T announced that it has developed a security chip to protect data stored on computer disks, in cellular phones, and television set-top boxes all of which will utilize the Clipper chip.[142] With the simplicity of an Executive Order, the President could strongly recommend for all executive agencies to conduct communications utilizing a key recovery system. Any secure communication with a government agency would then have to be conducted utilizing the government accessible key recovery system. This saturation would allow the government mandated key recovery system to become the de-facto standard and destroy the concept of independent encryption that does not support key recovery. In fact, the former General Counsel of NSA recently admitted that "[t]he [government's] concern . . . is the prospect that in five years . . . every phone you buy that costs $75 or more will have an encrypt button on it that will interoperate with every

maximum limit and communicated to another country or foreign embassy, then NSA has jurisdiction based on the fact that there has been a violation of the ITAR by exporting without a proper license. But in a recent interview with a government official, it was unclear under what authority NSA has authority when it conducts eavesdropping of foreigners who communicate with the use of encryption within the United States. Interview with an anonymous intelligence government official, in Washington, D.C. (Oct. 11, 1996) (notes on file with the COMMLAW CONSPECTUS).

131 Hanson, *supra* note 129, at 14.

132 *Id.*

133 *Id.*

134 Dorothy Denning, *Clipper Chip will Reinforce Privacy*, WASH. TIMES, Oct. 24, 1994, at 18.

135 *See* Froomkin, *supra* note 10.

136 *Impact of Emerging Telecommunications Technologies on Law Enforcement* (visited Jan. 25, 1997) <http://epic.org/crypto/ban/fbi_dox/impact_text.gif>.

137 *Encryption: The Threat, Applications and Potential Solutions* (visited Jan. 25, 1997) <http://epic.org/crypto/ban/fbi_dox/mandatory.gif>.

138 The U.S. government is the largest purchaser of telecommunication products in the world. Sean Flynn, *A Puzzle Even the Codebreakers Have Trouble Solving: A Clash of Interests Over the Electronic Encryption Standard*, LAW AND POLICY IN INT'L. BUS., Sept. 22, 1995, at 220.

139 Levy, *supra* note 34, at 7.

140 Edmund Andrews, *U.S. Plans to Push Giving F.B.I. Access in Computer Codes*, N.Y. TIMES, Feb. 5, 1994, at F1.

141 Murray Slovick, *The Big Brother Chip: Clipper Data-Encryption Chip*, POPULAR MECHANICS, Sept. 1994, at 117.

142 *1995: Year in Review*, MULTIMEDIA & VIDEODISC MONITOR, Feb. 1, 1996, at 22.

other phone in the country . . ."[143] The question then truly becomes, is voluntary really voluntary?

III. THE OTHER SIDE: INDIVIDUAL AND INDUSTRY'S INTEREST IN THE CRYPTO DEBATE

Unbreakable encryption is of interest to anyone who uses the Internet to conduct affairs. A number of recent events have attributed to a wave of concern over the lack of secure communications. In September 1994, a group of hackers penetrated the National Weather Service computer network in Maryland, but were stopped before any damage was done.[144] If the hackers had caused the weather service's computer to shut down, then all commercial airlines, who are dependent upon its information, would have been grounded as a result.[145] In October 1994, a sixteen year-old hacker was arrested after breaking into over 100 networked systems, including the South Korean Atomic Energy Research Institute, where it was acknowledged that he may have accessed some secret nuclear data.[146] Also, in August 1996, hackers altered the Justice Department's web site so that it read: "United States Department of Injustice" and placed several swastikas placed on the page.[147]

Legal testing of the protection afforded by encryption devices also creates alarm. In early 1994, after only eight months, a team led by Bell Labs, working with 600 volunteers in twenty-four countries cracked a 129 bit key.[148] Before the results of this test, scientists had asserted that a 129 bit key was uncrackable for forty quadrillion years.[149] A recent study conducted by cryptographers also concluded that "uncrackable" keys did not exist.[150] With the use of a $200 Field Programmable Gate Array (FPGA) chip, an individual could crack a 40 bit key in 5 hours.[151] With the resources of $10 million, a 56 bit key could be penetrated in six minutes; with $300 million it would only take twelve seconds.[152] The authors also point out that these figures are not static since computing power doubles every eighteen months.[153] Therefore, in the two year time period established by the Clipper III proposal, this figure will have more than doubled. At first glance, these dollar figures might seem enormous, but to many corporations and governments, they represent only a drop in the bucket. The report concludes that in order to have adequate protection for the next twenty years, a system should use a key at least ninety bits long.[154] All of these cases illustrate the fragility of existing electronic networks. Yet, the government continues to advocate the voluntary implementation of a de-facto standard of encryption technology based on key recovery in order to protect its law enforcement capabilities.

A. Past Abuses in the Name of National Security

Critics of governmental control of the encryption debate also express concern about the poten-

---

143 Stuart Baker, General Counsel of NSA, Remarks at the Fourth Annual Conference on Computers, Freedom and Privacy, session entitled "Data Encryption: Who Holds the Keys?" at the John Marshall Law School, Chicago (Mar. 24, 1994) (visited Jan. 25, 1997) <http://www.cpsr.org/dox/conferences/cfp94/encpanel.html/>.

144 Joseph C. Panettieri, *Are Your Computers Safe?*, INFO. WK., Nov. 28, 1994, at 34, 42.

145 *Id.*

146 *Id.* at 42, 46. In November 1994, an MCI employee was charged with stealing 100,000 telephone calling card numbers which were subsequently used to place $50 million worth of long distance calls. *Id.* at 46. In February 1995, Kevin Mitnick was arrested for stealing 20,000 credit card numbers and billions of dollars worth of corporate information by tapping into electronic networks. Della de Lafuente, *Loyola U. Plays Role in Tracking Wanted Hacker*, CHI. SUN TIMES, Feb 17, 1995, at 49. In September 1995, a computer hacking ring led by a Russian biochemistry student hacked into Citicorp's $500 billion-a-day network and transferred $11 million into their accounts and withdrew a total of 400 thousand dollars. *All Things Considered*, NATIONAL PUBLIC RADIO, Sept. 16, 1995 (transcript on file with COMMLAW CONSPECTUS).

147 *Vandals Show Justice's Vulnerability*, DAYTON DAILY NEWS, Aug. 24, 1996, at 11A.

148 Ellen Messmer, *Bellcore Leads Team Effort to Crack RSA Encryption Code*, NETWORK WORLD, May 2, 1994, at 14. Even more startling, was that the team leader asserted that the process would have only taken eight weeks, had all of the computers been in the same room.

149 *Id.*

150 Matt Blaze, *supra* note 10. The authors include Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson and Michael Wiener. The paper focues only on symmetric crypto-systems and not the asymmetric or public key crypto-systems. However, the paper points out that public key crypto-systems "are subject to shortcut attacks and must therefore use keys *ten or more times* the lengths of those discussed here to achieve the an (sic) equivalent level of security." *Id.* (emphasis added).

151 *Id.*

152 *Id.*

153 *Id.*

154 *Id.*

tial for abuse. The government has repeatedly assured the public that fears of escrow and recovery abuse are unwarranted. It proposes safeguard procedures, such as the requirement of a court authorization, which would protect against any form of abuse, from either the government or private sector.[155] However, if history is a reliable indicator, there is genuine cause for concern.

During the '50s, the FBI identified 26,000 "potentially dangerous" persons who would be rounded up in the event of a national emergency.[156] The CIA, from 1953 to 1973, opened and photographed 250,000 first class letters within the United States in order to compile a list of 1.5 million names.[157] During the '40s, based on illegal information provided by the Census Bureau, 112,000 Americans of Japanese ancestry were put in internment camps.[158]

While in office, President Kennedy ordered illegal wiretaps of citizens, including a former FBI agent and a newspaper reporter.[159] As recently as April 1996, several Social Security workers gave confidential information on at least 11,000 people to a credit card fraud ring, which resulted in at least $330,000 in unauthorized charges.[160] The government asks the public to trust it with access to the keys to all phone and data forms of communication. Yet, based on the evidence of past abuses, the creation of a system where such an invaluable prize can be claimed by the possessor of this information, abuse and corruption in some form, is certain.

B. An International Market That Must Be Guided by an International Community

The business community expresses concern that government-controlled encryption ignores international market concerns. The computer revolution has brought about numerous new and innovative possibilities in helping to reshape our society. One possibility that remains to be fully discovered is electronic commerce. The development of "cybercash" or international currency has the potential of opening doors that were never dreamed of being opened.[161] With the capabilities of the Internet and the concept of cybercash protected by strong encryption, one could instantly download a copy of the most recent book in Bangladesh. However, without the security of strong encryption, the distributor of the book might as well put it on a bulletin board.

The fear of manipulation or duplication of one's product has at least partially resulted in abysmal sales of only $350 million over the Internet, as compared with $53 billion spent on catalog shopping.[162] The need for protection is evidenced by the abuse that is currently taking place on the Internet. On one occasion, a student's computer became a "swap shop" of copyrighted software. The government estimates that in a very brief period of time, a total of over $1 million worth of copyrighted material was downloaded.[163] Entire texts of books have appeared on the Internet,[164] prompting numerous copyright concerns.[165] Encryption could help producers to receive authenticated orders from consumers. They then could fill the order by transmitting the encrypted product, which would be safe from manipulation, to the consumers. Existing technology would provide protection against any unauthorized duplication.

As of 1991, the encryption market in the United States was $384 million. By the end of

---

155 *See generally*, Froomkin, *supra* note 10.

156 *Id.* at 732 (quoting S. REP. NO. 94-755, pt. 2, at 4 (1976)).

157 *Id.*

158 Susan Landau, *Crypto Policy Perspectives*, COMM. OF THE ACM, Aug. 1994, at 115, 119.

159 Timothy Lennon, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 be Like 1984?*, 58 ALB. L. REV. 467, 475 (1994) (quoting David Wise, *The American Police State: The Government Against the People* at 66 (1978)).

160 Saul Hansell, *U.S. Workers Stole Data on 11,000, Agency Says*, N.Y. TIMES, Apr. 6, 1996, at A6. Another example of abuse occurred when in October 1992, over three hundred employees of the Internal Revenue Service were identified as using one of the computers to issue fraudulent refunds and to browse through taxpayer accounts. U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS, OTA-TCT-606 (Washington, D.C.: U.S. Gov't Printing Office, Sept. 1994) at 3.

161 *Net Profits*, ECONOMIST, July 1, 1995, at 12.

162 Ken R. Wells, *Transactions Over the Internet Safe Despite Publicized Thievery*, SAN DIEGO BUS. J., Feb. 5, 1996, at 15.

163 *Nightline: Law and Order on the Information Superhighway* (ABC television broadcast, May 2, 1994) (report concerning David LaMacchia, who established a computer bulletin board which contained copyrighted software available for download) (transcript on file with COMMLAW CONSPECTUS).

164 Carolina Saez, *Enforcing Copyrights in the Age of Multimedia*, 21 RUTGERS COMPUTER & TECH. L.J. 351, 381-82 (1995).

165 *See generally*, Dale J. Ream, *Copyrighted Works & Computer Networks: Is Protection Possible?*, 4 KANSAS J.L. & PUB. POL'Y 115 (1995); Kenneth D. Susan, *Tapping to the Beat of a Digital Drummer*, 59 ALB. L. REV. 789 (1995).

1996, that figure is estimated to climb to $946 million.[166] This figure is properly analyzed when taken in conjunction with the fact that this accounts for less than fifty percent of the total worldwide encryption market.[167] American manufacturers place primary blame for the sizable foreign-market share on the existence of the restrictive export regulations placed upon U.S. technology. Other countries, such as Japan, Russia, Germany, France and the U.K., produce and export encryption of a fifty-six-bit key strength and higher.[168] Senator Leahy recently stated that, "U.S. companies are not allowed to market globally the one encryption method that's used around the world."[169] Therefore, U.S. software companies must choose between what type of lines to produce. A company could produce one line at forty key bits which is exportable or a company could produce two different lines of the same product, one which is exportable and the other not. Due to the cost prohibitive nature of maintaining two different lines of the same product, most U.S. companies opt to produce one weakly encrypted exportable line. The effects of this policy have proven financially disastrous. This backwards standard will cost U.S. software companies $6 billion to $9 billion in annual revenues.[170] This figure is expected to rise to $60 billion in annual revenues by the year 2000.[171]

One computer company reported that it lost sales of $70 million because it was not able to provide the encryption that its customers wanted.[172] For the companies that choose to market two different lines, the results are the same. An example of this occurred in France where a hacker using two supercomputers and 120 workstations was able to crack the non-U.S. version of Netscape.[173] A CEO of a computer company put it best when he responded to a question concerning the Clipper by stating, "Why would an international company want the U.S. government to be able to eavesdrop on them?"[174] The irony of the situation is further exemplified by the fact that three out of ten Fortune 500 companies already rely on stronger foreign encryption products.[175]

Economic espionage resulting in the theft of technology and trade secrets has become one of the biggest concerns among the business industry. A former CIA Director called this form of spying "the hottest current topic in intelligence."[176] Experts estimate that anywhere between $20 to $30 billion a year is lost by American business as a result of foreign and domestic spying.[177] Out of the twenty foreign governments that are often cited as supporting campaign of economic espionage against the U.S. business community, the most frequently mentioned are France and Japan.[178] In the spring of 1993, the CIA obtained a list of technologies allegedly sought by France, naming forty-nine manufacturers and twenty-six financial firms and U.S. government laboratories and agencies.[179] Also in 1993, the FBI reported that its caseload of industrial espionage increased from ten to five hundred in a period of nine months.[180] NSA and other U.S. intelligence agencies have been slow in taking any form of affirmative action against the foreign governments, let alone acknowledging the existence of the problem. This inaction stems from the fact that the U.S. intelligence agencies conduct many of the same activities, and wish to continue doing so. As a result, U.S. businesses are being asked to continue making sacrifices for the betterment of various law enforcement and intelligence agencies.[181]

---

166 Hoffman, *supra* note 6.

167 *Id.*

168 *Id.*

169 National Information Infrastructure Copyright Protection Act of 1995: *Joint Hearing Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary and the Senate Comm. on the Judiciary*, H.R. 2441 and S. 1284, 104 Cong., 72 (1995) (statement of Sen. Leahy).

170 Fahys, *supra* note 2, at F1.

171 Christine Hudgins-Bonafield, *Will Spies Hold Your Keys*, NETWORK COMPUTING, Mar. 15, 1996, at 78, 79.

172 Aley, *supra* note 126, at 101.

173 Jeff Prosise, *The Netscape Security Breach*, PC MAG., Apr. 23, 1996, at 199, 200.

174 Aley, *supra* note 126, at 100.

175 Hudgins-Bonafield, *supra* note 171, at 82.

176 Thomas Omestad, *Cloak and Dagger as R&D*, WASH. POST, June 27, 1993, at C2.

177 Roderick P. Deighen, *Welcome to Cold War II*, CHIEF EXECUTIVE, Jan./Feb. 1993, at 42.

178 France is considered the most "brazen perpetrator," by breaking into Paris hotel rooms of foreign executives and bugging first-class cabin, on Air France. Japan's efforts are largely coordinated by the Ministry of International Trade and Industry, which obtains and analyzes vast amounts of publicly-accessible commercial information for Japanese companies. Omestad, *supra* note 176, at C2. One report estimated that the Ministry's Trade Organization files a total of 10,000 pages a day on the companies, governments and economies of the target countries as a "part of their normal business routine." Deighen, *supra* note 177, at 45.

179 Omestad, *supra* note 176, at C2.

180 *Id.*

181 The export restriction placed upon industry does

IV. THE THREE CRUSADERS FOR CONSTITUTIONALLY PROTECTED ENCRYPTION

Just within the last few years the judicial branch emerged as the forum for the cryptography debate. Three individuals, who wished only to share their encryption programs and ideas with the rest of the world, have brought the government to court. Their arguments are based primarily on the assertion that the source code used for encryption constitutes speech and therefore, should be afforded First Amendment protections. The government's response revolves around national security concerns. The Director of FBI Counter Intelligence, Edward Apell, recently stated that the wide distribution of encryption in either the form of a book or computer disk is a threat.[182] However, this statement appears to be contradictory to the government's position in *Karn v. United States Dep't of State.*[183]

A. Phil Karn

In 1994, Bruce Schneier wrote a book entitled "Applied Cryptography," which contained explanations of how to build cryptography into products, illustrates cryptographic techniques, evaluates algorithms and provides examples of some algorithms.[184] On February 12, 1994, a friend of Schneier by the name Phil Karn, a San Diego software developer, wrote to the State Department to ask whether a license was required to export the book.[185] One month later, a reply to the CJ Request stated that the book was not subject to the "licensing jurisdiction of the Department of the State since the item is in the public domain."[186] Since that time, the book has sold 25,000 copies in the United States and abroad.[187]

On March 9, 1994, just seven days after obtaining approval from the State Department for export of the book, Karn wrote to the State Department to ask whether a license was required to export a computer disk version of the same book.[188] The disk contained, line for line, the same source code listed in the book.[189] Two months later, the Office of Defense Trade Controls concluded that the computer disk was subject to the licensing jurisdiction of the State Department since it was determined that the computer disk was a defense article.[190] The same individual that made the decision regarding the export of the book stated that, "[t]he text files on the subject disk are not an exact representation of what is found in 'Applied Cryptography.' Each source code listing has been partitioned into its own file and has the capability of being easily compiled into an executable subroutine."[191] The distinction between the material in a book format versus an electronic format was further justified by the fact that it was of an "added value to the end-user that wishes to incorporate encryption into a product."[192]

The initial ODTC decision was subsequently appealed to the Secretary for Export Controls.[193]

---

have some exceptions. DES, 56 key bit encryption, is available for some banking and medical services. *See* King, *supra* note 13 at 231. Recently, Health Online Service, was awarded an export license of a 786 character encryption key software. *For Doctors Only*, LINK-UP, May/June 1996, at 8.

182 Interview by Dan Charles with Edward Apell, Diector, F.B.I. Counter Intelligence, *All Things Considered*, (National Public Radio, Sept. 28, 1995). The pertinent statements were made in response to questions concerning a book that contained the whole PGP program. He stated, "[i]t is a source code, it is a program. It instructs the computer. And if you can scan it into the computer; if you can use it to tell the computer what to do, then it is, in fact, a machine itself." *Id.*

183 Karn v. United States Dep't of State, 925 F. Supp. 1 (D.C. Cir. 1996).

184 Bruce Schneier, *Electronic Speech-for Domestic Use Only*, NETWORK WORLD, Jan. 16, 1995, at 29.

185 *ODTC Case: 038-94*, Letter from Phil Karn, to Major Gary Oncale, Office of Defense Trade Controls, Department of State (Feb. 12, 1994). When Phil Karn was asked the reason why he wished to export a book and disk he did not author he responded, "I see this as a good test case that shows just how silly the rules are." *Crypto Speech Case Heating Up*, VOORHEES REPORT, Dec. 9, 1994, at 3. This letter and all other relevant letters and pleadings related to this proceeding can be located at Phil Karn's web site: (visited Jan. 25, 1997) <http://www.qualcomm.com/people/pkarn/export/>.

186 *ODTC Case: CJ 038-94*, Reply Letter from William B. Robinson, Office of Defense Trade Controls, Department of State, to Bruce Schneier (Mar. 2, 1994).

187 Nathaniel Sheppard Jr., *U.S. Laws Take Bytes From Secret Code Book*, CHI. TRIB., June 8, 1995, at N24.

188 *ODTC Case: CJ 081-94*, Letter from Phil Karn, to Major Gary Oncale, Office of Defense Trade Controls, Department of State (Mar. 9, 1994).

189 *Id.*

190 *ODTC Case: CJ 081-94*, Reply Letter from William B. Robinson, Director of Office of Defense Trade Controls, Department of State, to Phil Karn (May 11, 1994).

191 *Id.*

192 *Id.*

193 *ODTC Case: 081-94*, Appeal of Commodity Classification from Phil Karn, to Dr. Martha Harris, Deputy Assistant Secretary for Export Controls, Department of State (June 7, 1994).

Karn argued that the alleged "added value" was a flawed argument. He asserted that through the use of optical character recognition (OCR) technology by scanning the text of chapter five of the book onto a computer, the same material in the exportable book was produced onto the unexportable computer disk. The only difference being the medium on which the material was presented.[194] Karn's arguments, however fell on deaf ears and the initial decision was affirmed.[195] Karn then appealed the decision to the Bureau of Political-Military Affairs at the Department of State, where it was again affirmed.[196]

On September 21, 1995, Karn advanced the argument that "the prior licensing requirement of the ITAR operates as a prior restraint on Plaintiff's disclosure of ideas and information in violation of his First Amendment rights (sic) to free speech" in a United States District Court.[197] He reiterated the argument that there was no difference between the information on the book and the information on the computer disk, other then the medium itself.[198] Karn pointed out that the computer disk also contained "comments" that were not involved in the functioning program, in addition to the source code, which was further evidence of its "communicative purpose."[199]

The government contended that "designation of encryption software on the USML is unrelated to any expressive value"[200] and the "crucial" governmental interest of "national security," which the court was "precluded from second guessing."[201] The government further contended that the encryption program could not be viewed as "convey[ing] a particularized message," and as such the First Amendment claim must fail.[202] Assuming that the conduct was "expressive conduct," which was afforded constitutional protection, the government argued that the *O'Brien* test should be applied.[203] In applying the *O'Brien* test, the government argued that the disk was not regulated for its "informational or expressive value . . . but because of its functional use."[204] The government asserted that the well-defined distinction between the book and the computer disk, was in its "function" or "the capability to provide to whomever obtains it."[205] Yet at the same time, in what would appear to be a contradictory argument, the government concluded that the fact that the encryption source codes may be scanned onto a computer disk may "compel reconsideration of the status of the printed source codes . . . ."[206] It appears the government's attorneys neglected to confer with the Director of FBI Counter Intelligence before reaching this conclusion.

On March 22, 1996, the court granted the Defendant's Motion for Summary Judgment in part with respect to the plaintiff's First Amendment claims.[207] The court held that the defendants were not regulating the export of the disk because of the "expressive content of the comments and

194 *Id.*

195 *ODTC Case: 081-94*, Reply Letter from Dr. Martha Harris, Deputy Assistant Secretary for Export Controls, Department of State, to Phil Karn (Oct. 7, 1994)

196 *ODTC Case: 081-94*, Letter from Kenneth C. Bass, III and Thomas J. Cooper, representing Phil Karn, to Thomas E. McNamara, Assistant Secretary of the Bureau of Political-Military Affairs, Department of State (Dec. 5, 1994). The decision was, *ODTC Case: 081-94*, Reply Letter from Thomas McNamara, Assistant Secretary of the Bureau of Political-Military Affairs, Department of State, to Phil Karn (June 13, 1995).

197 Complaint at 7, Karn v. United States Dep't of State, 925 F. Supp 1, (D.C. Cir. 1996).

198 *Id.* at 5.

199 Plaintiff's Opposition to Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment at 10, 925 F. Supp.

200 Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss or in the Alternative, for Summary Judgment at 34, *Karn*, 925 F. Supp. 1 (quoting Texas v. Johnson, 491 U.S. 397, 403 (1989).

201 *Id.* at 4.

202 *Id.* at 19-20.

203 *Id.* at 20. The four-part *O'Brien* test is: (1) it is within the constitutional power of the Government, (2) it furthers an important or substantial government interest, (3) the governmental interest is unrelated to the suppression of free expression, (4) the incidental restriction on the alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest. United States v. O'Brien, 391 U.S. 367, 377 (1968).

204 Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss or, In the Alternative, for Summary Judgment at 27, *Karn*, 925 F. Supp. 1.

205 *Id.* at 3.

206 *Id.* at 28. The government contended, due to the lack of perfection of OCR technology, it did not yet produce error-free reproductions. Any errors that were made would necessitate the need for an individual with knowledge to remedy the situation. In the case of a preprogrammed computer disk, very little knowledge of the encryption technology is needed. Concerning the technology of OCR, a recent newspaper article reported that there are currently a number of businesses in the Pacific Rim and other Asian countries that specialize in scanning vast amounts of text onto computers. *See* Sheppard, *supra* note 187.

207 *Karn*, 925 F. Supp. 1, *appeal docketed*, No. 96-5121 (D.C. Cir. Sept. 20, 1996).

or source code, but instead are regulating [it] because of the belief that the combination of encryption source code on machine readable media will make it easier for foreign intelligence sources to encode their communications."[208] Therefore, the court concluded that the regulation was "content neutral" and the *O'Brien* test should be applied.[209] Relative to whether the regulation is within the power of the government and whether it furthers a significant governmental interest, the court stated that it "*will not scrutinize the President's foreign policy decision*" and the court 'neither has the aptitude, facilities, nor responsibility' to make a judicial decision of this kind.[210] The last test, whether the regulation is "narrowly tailored to the goal of limiting the proliferation of cryptographic products," was dismissed by the court because of the plaintiff's failure to "articulate any present barrier to the spreading of information on cryptography 'by any other means,' other than those containing encryption source code on machine-readable media."[211] Interestingly enough, this last argument addressed by the court is one of the very issues in dispute in the next two cases.

B. Daniel Bernstein

In 1992, Daniel Bernstein, then a graduate student of the mathematics department at the University of California at Berkeley, developed an encryption algorithm named "Snuffle."[212] In an effort to continue his research, Bernstein wished to publish his discovery in a paper and a computer program which implements the algorithm. He also sought to post his encryption program and related documents upon an Internet discussion group called "sci.crypt." Aware of the export restrictions, Bernstein filed a request with the State Department so that he would be able to export his paper and computer disk.[213] The State Department responded that he would need a license.[214] However, in an attempt to allow the government to separately consider each item, Bernstein filed five separate requests with the State Department.[215] The State Department responded by consolidating the items into one request and summarily asserting that a license was needed.[216] The supporting rationale was that the "referenced items contain cryptographic source code for data encryption and are used in a stand-alone cryptographic product."[217]

Two years later, on February 21, 1995, Bernstein brought suit against the federal government. The complaint asserted that the export regulations in question are "unlawful prior restraints depriving them [Bernstein and other academics] of their federal constitutional rights to speak, to publish, to assemble, to receive information and to engage in academic study, inquiry and publication, guaranteed by the First Amendment."[218] In particular, Bernstein argued that the three step licensing process and the approval process effectively "prevents general publication."[219] Bernstein contended that as a student of science, the lack of an exchange of information or ideas infringed on his "right of academic freedom."[220] He also argued that computer software is simply another language and the Court should not allow the government "to force him [Bernstein] to publish it only in the languages they [the government] choose (English, as opposed to computer languages)."[221]

---

208 *Id.* at 10.

209 *Id.*

210 *Id.* at 11 (quoting Chicago & Southern Air Lines v. Waterman SS. Corp., 333 U.S. 103, 111 (1948) (emphasis added)).

211 *Id.* at 12.

212 *Bicoastal Court Challenges: Tackling Export Controls on Encryption*, LEGAL TIMES, Oct. 30, 1995, at 2.

213 *See ODTC Case: 191-92*, Letter from Daniel Bernstein, to Office of Defense Trade Controls, Department of State (June 30, 1992). All documents related to Bernstein's requests and subsequent litigation are at: (visited Jan. 25, 1997) <http://www.eff.org/pub/Privacy/ITAR_export/Bernstein_case/Legal/>.

214 *ODTC Case: 191-92*, Reply Letter from William Robinson, Director of Office of Defense Trade Controls, Department of State, to Daniel Bernstein (Aug. 20, 1992).

215 Complaint at 17, Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D.Cal. 1996); The five requests included: (1) a scientific paper entitled "The Snuffle Encryption System;" (2) source code for the encryption component of Snuffle; (3) source code for the decryption component of Snuffle; (4) a description of how to encrypt using Snuffle; (5) instructions for programming a computer to use Snuffle. *Id.*

216 *ODTC Case: 214-93*, Reply Letter from William Robinson, Director of Office of Defense Trade Controls, Department of State, to Daniel Bernstein (Oct. 5, 1993).

217 *Id.*

218 Complaint at 25, Bernstein, 922 F. Supp. 1426 (N.D. Cal. 1996).

219 Plaintiff's Opposition to Motion to Dismiss at 9, *Bernstein*, 922 F. Supp. 1426.

220 Complaint at 43, *Bernstein*, 922 F. Supp. 1426.

221 Plaintiff's Opposition to Motion to Dismiss at 22, *Bernstein*, 922 F. Supp. 1426.

The government promptly filed a motion to dismiss where it was argued that the issue was the "exportation of actual cryptographic software" and not the "academic discussion about its underlying theory."[222] It was contended that the source code is not speech but simply "mathematical ideas expressed in computer language."[223] The fact that these ideas provide a recipient with all of the necessary facilities to "function[ly]" encrypt data makes them distinct from an explanation or discussion about the "science of cryptology." Therefore, the government argues that the court may not "second guess" the USML designation of cryptographic software.[224]

On April of 1996, U.S. District Judge Marilyn Hall Patel denied the government's motion to dismiss.[225] In dismissing the government's motion, the court was the first court to ever hold that the source code is protected as speech under the First Amendment. It was asserted that there "was no meaningful difference between computer language. . .and German or French."[226] Concerning the functionality aspect of the source code, the court held that it "does not remove it from the realm of speech . . . [i]nstruction, do-it-yourself manuals, recipes and even technical information about hydrogen bomb construction . . . are often purely functional: they are also speech."[227] The final outcome of this case has the opportunity of establishing original precedent in an area that is, as one former Justice Department official remarked, of "huge significance because the government's ability to police its borders for control of export of high-tech munitions hangs in the balance."[228]

C. Peter Junger

The third case to question the constitutionality of the restrictions on the export of encryption was filed by a law professor from Case Western University Law School by the name of Peter Junger.[229] The subject of the dispute revolves around Professor Junger's class entitled "Computers and the Law."[230] In May 1993, Prof. Junger wrote an encryption program that he wished to present to his class.[231] Concerned of the implications of distributing the program and related information to foreign students, Prof. Junger contacted the Department of Commerce, Department of State, the ODTC and NSA in hopes of determining whether his program was subject to export regulations.[232] After numerous contacts with the various agencies, he was unable to obtain a determinative answer.[233] Three years later, Prof. Junger filed a federal suit against the State Department and National Security Agency.

Professor Junger's main contention is that the "[ITAR] regulations are unconstitutional because they constitute a blatant system of overbroad and vague prior restraints that violate rights of academic freedom of association."[234] As a result of the restrictions, Prof. Junger argues that he must chose "between petitioning the government and allowing foreign students in his class."[235] It is further asserted that the ITAR serves as a "prepublication licensing scheme" and as such, the law demands that procedural safeguards be in place.[236]

---

222 Reply Memorandum of Points and Authorities in Further Support of Defendants' Motion to Dismiss at 11-12, *Bernstein*, 922 F. Supp. 1426.

223 *Id.* at 12.

224 *Id.* at 6.

225 *Bernstein*, 922 F. Supp. 1426.

226 *Id.* at 1435.

227 *Id.*

228 LEGAL TIMES, *supra* note 212.

229 Junger v. Christopher, (No. 96 CV 1723) (N.D. Ohio Aug. 7, 1996). All documents and pleadings concerning this case can be found at: (visited Jan. 25, 1997) <http://samsara.law.cwru.edu/comp_law/jvc/index.html>.

230 Complaint at 2, *Junger*, (No. 96 CV 1723) (N.D. Ohio filed Aug. 7, 1996).

231 *Id.* at 2-3.

232 *Id.* at 3.

233 Brief in Support of Plaintiff's Motion for Preliminary Injunction at 5, *Junger*, (No. 96 CV 1723) (N.D. Ohio Aug. 7, 1996). When Prof. Junger's attorney was questioned why his client did not file a Commodity Jurisdiction (CJ) Request to obtain a definitive answer from the ODTC, he responded by stating that it "would not be practical; because he has a lot of information that he wishes to distribute . . . and he would end up spending all of his time filling out CJ requests. In addition, we don't have to get a permit to make a First Amendment claim." Telephone Interview with Gino Scarselli, Attorney for Professor Junger (Oct. 10, 1996). It is foreseeable that the government may use this information to argue that Prof. Junger's claim is not ripe because no request was ever made and as a result, there may be no issue to dispute. As support for the government's contention the Supreme Court has asserted that the "exhaustion doctrine continues to apply as a matter of judicial discretion in cases not governed by the APA." Darby v. Cisneros, 509 U.S. 137, 153-54 (1993).

234 Brief in Support of Plaintiff's Motion for Preliminary Injunction at 11-12, Junger v. Christopher, (No. 96 CV 1723) (N.D. Ohio Aug. 7, 1996).

235 *Id.* at 13-14.

236 *Id.* at 15; *see* Freedman v. Maryland, 380 U.S. 51 (1965).

Another key argument raised in the brief is that First Amendment protection should be afforded to Prof. Junger's program because "even executable programs in machine code, are afforded copyright protection."[237] Undoubtedly, this argument was based in part on the fact that Judge Patel in the Bernstein litigation had subscribed to the same reasoning when she asserted that "the expression of an idea" is afforded copyright protection.[238] Therefore, Judge Patel reasoned that "[a]n encryption program expressed in source code communicates to other programmers and ultimately to the computer itself how to make the encryption algorithm (the idea) functional" and as a result, "copyright law does lend support to the conclusion that source code is a means of original expression."[239]

In the *Junger* case, the government reaffirms its argument that the "controls are expressly linked to the *capability* of the product, not the content of ideas or speech."[240] As a result, the government contends that the court should examine the regulations as content neutral.[241] However, one can infer quite the contrary, when the government, several paragraphs later, states the purpose of the export controls is to limit the spread of a product that can encrypt data.[242]

The government also asserts that the "broad public exchange of information . . . [through] [a]cadmeic teaching, publication, research and symposia" serves as evidence that the government is not interested in the spread of ideas at home, but at the spread of encryption software overseas.[243] In regards to the software itself, the government contends that it "is not merely 'know how' that explains how cryptography works, or a description of scientific ideas or information related to cryptography."[244] Rather, the government asserts that the software "enables a computer to perform a cryptographic function" and the regulation therefore only goes to the "functionality" of the software.[245]

Even with the recent announcement of the Clipper III initiative and the transfer of export control over to the Commerce Department, these three cases still present First Amendment issues that remain unresolved. Until such time that the administration or the courts recognize that encryption is speech and afford it speech status with the appropriate First Amendment protections, these cases represent the only hope for the future of encryption-speech.

V. ANALYSIS OF FIRST AMENDMENT IMPLICATIONS

Regardless of the outcome and implementation of the Clipper III initiative, it can be argued the government has failed to recognize that source code is speech and should be afforded the first amendment protections. As a result, the ongoing litigation of the three aforementioned cases are necessary in order to confront the administration's attempt to window-dress key escrow as key recovery. Only after source code has been held to be speech will the future forms and mediums of communication be protected. The next section will present an analysis of the constitutional issues and questions raised by recognizing that encryption and specifically, source code is speech under the First Amendment.

A. Source Code is Speech

As previously discussed, source code is used in the process of encrypting and decrypting commu-

---

237 Brief in Support of Plaintiff's Motion for Preliminary Injunction at 18-19, Junger, (No. 96 CV 1723) (N.D. Ohio Aug. 7, 1996).

238 Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996).

239 *Id.*

240 Defendants Memorandum of Point and Authorities in Opposition to Plaintiff's Motion for a Preliminary Injunction and in Support of Defendant's Motion to Dismiss or in the Alternative, for Summary Judgment at 19, Junger v. Christopher, (No. 96 CV 1723) (N.D. Ohio Aug. 7, 1996) (emphasis added).

241 *Id.* at n.24. *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622 (1994); City Council v. Taxpayers for Vincent, 466 U.S. 789, 810 (1984).

242 Defendant's Memorandum *supra* note 240, at 20. This statement seems to suggest that, in reality, the government's desire to control the "spreading" of a product that has the capability to encrypt, is in actuality an agenda to control the content of the program that allows the product to perform the task. Therefore, the government's contention that the regulation is content neutral is a misplaced attempt to force the court to examine the form and not the substance of the encryption product.

243 *Id.* at 13.

244 *Id.* at 22.

245 *Id.* at 22-23. The government's assertion, by singly concentrating on one character of the software, blindly ignores all of the other different aspects of the software. It should be noted that all of these additional qualities that the government has chosen to ignore go directly to the content of the software.

nication. In order to determine if source code is protected under the First Amendment, it must first be determined whether source code is speech within a first amendment context.[246] From its inception to present day, the First Amendment has been applied to a variety of different mediums. Newspapers, leaflets, pamphlets, films, and broadcasting have all been recognized by the Supreme Court as qualifying for first amendment protection.[247] In analyzing the many different mediums, the Court has held that, "[t]he press in its historic connotation comprehends every sort of publication which affords a vehicle of information and opinion."[248] The freedom to express one's ideas has long been recognized as one of the founding principles for the existence of the First Amendment.[249] This "marketplace of ideas" allows for the scholarly exchange of beliefs and ideas to separate the truth from the falsity. The Court recognized that academics serve an instrumental role in this process when it stated that, "[t]o impose any strait jacket upon the intellectual leaders in our colleges and universities would imperil the future of our Nation."[250]

Cryptography is a recognized science of mathematics that is taught at many educational institutions throughout the country. It is the science of using mathematical equations to create another form of communication, namely algorithms. A counter argument often asserted is that cryptography is not speech, because it provides a "function" and does not "convey a particularized message."[251] However, it should be argued that encryption algorithms are no different from a chemical equation, genetic code or even a nuclear fission equation.[252] All of these particular subjects would most likely be unintelligible to those that are not completely familiar with them, but that in itself does not strip them of any characteristics of protected speech.

Source code can also be compared to the protection afforded foreign languages. The Supreme Court has held that the First Amendment prohibits the government from restricting languages taught or used.[253] In *Yniguez*, the Court stated that "[s]peech in any language is still speech . . . ."[254] Therefore, the use of the computer language as a form of expression of ideas and information should be afforded the First Amendment protection that every other "foreign" language is afforded.

B. Government's Argument for Expressive Conduct

The government has also advanced the argument that source code is not speech but rather "expressive conduct."[255] The contention is that the algorithm contains non-speech elements which are combined with incidental speech elements and as such, a different test, the *O'Brien* test, should be applied.[256] This argument was recognized as flawed in *Yniguez*, where the court as-

246 Although neither *Karn* nor *Bernstein* reached a final disposition, each have arrived at a different conclusion regarding this issue.

247 CBS v. Democratic Nat'l Comm., 412 U.S. 94 (1973) (broadcasting); Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495 (1952) (motion pictures); United States v. Paramount Pictures, Inc., 334 U.S. 131 (1948) (motion pictures, newspapers, radio); Lovell v. City of Griffin, 303 U.S. 444 (1938) (pamphlets and leaflets).

248 *Lovell*, 303 U.S. at 452.

249 Abrams v. United States, 250 U.S. 616, 625 (1919) (Holmes J., dissenting).

250 Sweezy v. New Hampshire, 354 U.S. 234, 250 (1957) (noting the importance of protecting scholarship and academic inquiry); *see also* Kleindienst v. Mandel, 408 U.S. 753, 762-63 (1972) (recognizing that the First Amendment protects the right to receive information and ideas).

251 Texas v. Johnson, 491 U.S. 397, 404 (1989).

252 *Compare* United States v. Progressive Inc., 467 F. Supp. 990 (W.D. Wis. 1979) (holding that prior restraint was allowed on technical information about hydrogen bomb construction).

253 Meyer v. Nebraska, 262 U.S. 390 (1923); Bartels v. Iowa, 262 U.S. 404 (1923); Yu Cong Eng v. Trinidad, 271 U.S. 500 (1926); Farrington v. Tokushige, 273 U.S. 284 (1927).

254 Yniguez v. Arizonans, 69 F.3d 920, 936 (9th. Cir. 1995), *cert granted* 116 S.Ct. 2495 (1996).

255 *Id. supra* note 204, at 20.

256 Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss or, In the Alternative, for Summary Judgment at 27, Karn v. United States Dep't of State, 925 F. Supp 1, (D.C. Cir. 1996) (laying out the test). The government has also argued that a First Amendment attack is precluded based upon a 9th Circuit decision. Defendant's Memorandum of Point and Authorities in Support of Defendant's Motion for Summary Judgement at 7, Bernstein v. United States Dept' of State, 922 F. Supp. 1426 (N.D. Cal. 1996) (citing United States v. Edler Indus., 579 F.2d 516 (9th Cir. 1978)). The *Bernstein* court dismissed the defendant's argument "that if Edler allows the government to legitimately restrict the export of technical data relating to a defense article, it can certainly restrict the defense article itself." *Bernstein*, 922 F. Supp. at 1437. The court reasoned that the defendant's argument was an extension of the of the Edler decision that the court was "unwilling to adopt" based on the fact that the "validity of the scope of the munitions list was simply not an issue in that case." *Id.*

serted that all speech has elements of expressive conduct.

speech in any language consists of the 'expressive conduct' of vibrating one's vocal chords, moving one's mouth and thereby making sounds, or of putting pen to paper, or hand to keyboard. Yet the fact that such 'conduct' is shaped by a language - that is, a sophisticated and complex system of understood meanings – is what makes it speech. Language is by definition speech, and the regulation of any language is the regulation of speech.[257]

However, if the court should accept the argument that source code is not speech but rather only expressive conduct, then the court must apply the *O'Brien* test. The first prong of the four part test is whether the government's interest is unrelated to the suppression of free expression.[258] One government argument advanced is that their interest is only the "functional use" and not the scientific ideas. Applying this reasoning, the government argues that a book containing the same information as a computer disk is not as functional. This argument fails to acknowledge that the functionality of something is based upon the knowledge of the reader. For instance, if a graduate student studying cryptography at a university in Berkeley received a copy of an algorithm in a textual format, its functional value would be identical to the same information in a computer format. The same analogy can be applied to any other subject of information. If a political scientist received statistical information in textual format, its functional value would be identical to the same information compiled on a computer disk.

For one with a limited knowledge of a subject, the different formats, in either a book or computer disk, would make absolutely no difference to their functional values. It is argued that if an individual without the requisite knowledge comes across a problem while utilizing the textual format of the source code, it will be more of a formidable task to remedy the situation, compared to the limited knowledge necessary to operate the computer format. Therefore, the government's interest in preventing the "functional use" is literally a government interest in preventing the advantages of the information from being readily available in a format where an understanding of the information is not necessary. Limiting the extent of broadening one's knowledge has been held by the Supreme Court as "inconceivable" to "serv[ing] the public welfare or add[ing] substantially to the security of life, liberty or the pursuit of happiness."[259] The government's reasoning can not be supported and the only rational government interest is the suppression of free expression. As a result, the government fails the *O'Brien* test.

If the court should nevertheless accept that the government's interest as unrelated to the suppression of free expression, the government must still meet the second prong of the *O'Brien* test, which states that the regulation must further an important or substantial governmental interest.[260] The government has asserted that its interest is in "protect[ing] critical foreign intelligence gathering functions"[261] and "controll[ing] the foreign availability of a commodity that can . . . encrypt."[262] The government has based its conclusion upon information from NSA, which asserts that, "the proliferation of such products will make it easier for foreign intelligence targets to deny the United States access to information vital to national security interests."[263] The courts have also held "that no government interest is more compelling than the security of the Nation."[264]

It should be argued that in order to conduct a proper analysis of this prong of the *O'Brien* test, the arguments advanced by the government, one must focus on the word "furthers." The government alleges that controlling the increase of encryption is an important interest; yet the existence of hundreds of encryption products in foreign countries has not brought about any modifications to the U.S. domestic encryption policy. This approach has created a process where foreign cor-

257 *Yniguez*, 69 F.3d at 934-35.

258 O'Brien v. United States, 391 U.S. 367, 377 (1968).

259 Meyer v. Nebraska, 262 U.S. 390, 390 (1923).

260 *O'Brien*, 391 U.S. at 377.

261 Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss or, In the Alternative, for Summary Judgment at 21, Karn v. United States Dep't of State, 925 F. Supp. 1 (D.C. Cir. 1996).

262 Reply Memorandum of Points and Authorities in Further Support of Defendants' Motion to Dismiss at 12, Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D.Cal. 1996).

263 Memorandum of Points and Authorities, *supra* note 261, at 23.

264 Haig v. Agree, 453 U.S. 280, 307 (1981) (upholding passport revocation over a first amendment challenge); *but cf.* United States v. Robel, 389 U.S. 258, 264 (1967) (holding that "even the war power does not remove constitutional limitations safeguarding individual liberties").

porations are supplying the U.S. domestic market with encryption products. In fact, the number of foreign distributors has steadily increased and is expected to continue to rise if export regulations remain in place.[265] Therefore, it can be concluded that the export regulations do not control the proliferation or availability of encryption products, rather the regulations serve to deny only U.S. corporations wishing to distribute encryption products access to the worldwide market. As a result, the government argument should fail the second prong of the *O'Brien* test.

If the court should nevertheless accept that the government regulation does further an important or substantial interest, the government must still meet the third prong of the *O'Brien* test, which states that the "incidental restriction on alleged First Amendment freedom[s] is no greater than is essential to the furtherance of that interest."[266] The government asserts that this element is satisfied because the export of the software does not "preclude individuals from otherwise publishing or discussing scientific ideas related to . . . cryptographic algorithms."[267] However, the government does point out that the distribution of encryption on the Internet without "reasonable steps to confine the distribution of software to Internet sites within the United States" will result in a violation of the law.[268] As stated earlier, the government's only concern is with the functionality of the source code and not the scientific ideas. Therefore, the government contends that "ample alternative channels of communication" remain available.[269] The government also contends that cryptographic software that does not function to maintain secrecy, an example being software that functions to authenticate data, is not encompassed in the strict export regulations.[270]

It can be argued that the regulations do not provide for ample alternative channels for the communication of cryptographic subjects. The limitation of distribution on the Internet because the government believes that "making software available abroad has nothing to do with teaching a class"[271] is a grave misconception. In order for any theory to be properly tested, one must be afforded the opportunity to confirm his or her hypothesis. The hypothesis in the study of cryptography is that the source code, which is the heart of any algorithm, is effective at maintaining the integrity of the confidentiality of a communication. In order for this hypothesis to be effectively tested, one must be able to use the tools, the only tools which will allow the tests to be performed. The courts have held that the alternatives must be "sufficiently similar to the method foreclosed by the regulation."[272] The hypothesis must be scrutinized by many within the academic community before the hypothesis is considered factual and worthy of application. When the ability to effectively communicate is threatened, the regulation may be constitutionally inadequate.[273] The government's quashing of any substantive formulation of hypothesis, in effect, destroys the entire science of cryptography. As result, the government's policy is saying that you can study cryptography all you want, just don't produce any results. Therefore, based on the fact that the regulations remove ample alternatives to the study of cryptography, the government's arguments fail the third prong of the *O'Brien* test.

The fourth element of the *O'Brien* test whether

---

265 David Judson, *Senators Want to Open Export Market for Security Software*, GANNETT NEWS SERV., Mar. 5, 1996, at 1.

266 O'Brien v. United States, 391 U.S. 367, 377 (1968).

267 Defendant's Memorandum of Points and Authorities In Support of Defendant's Motion to Dismiss, or In the Alternative, For Summary Judgment at 33, Karn v. United States Dep't of State, 925 F. Supp. 1 (D.C. Cir. 1996).

268 Defendants Memorandum of Point and Authorities in Opposition to Plaintiff's Motion for a Preliminary Injunction and in Support of Defendant's Motion to Dismiss or in the Alternative, for Summary Judgment at 33, Junger v. Christopher, No. 96 CV 1723 (N.D. Ohio Aug. 7, 1996). The brief relies on the Declaration of William J. Lowell, the Director of the Office of Defense Trade Controls, Bureau of Political-Military Affairs, United States Department of State. It is important to note that the brief does not suggest what those "reasonable steps" are.

269 Ward v. Rock Against Racism, 491 U.S. 781, 802 (1989). The government has consistently argued that numerous channels currently exist. The existence of "courses on cryptography . . . routinely taught at dozens of colleges and universities . . . and several textbooks on cryptography [which] have been published over the years" serve as support for their assertion. Defendant's Opposition to Plaintiff's Motion for a Preliminary Injunction at 12, Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996).

270 *See* 22 C.F.R. § 167 (1996); 22 C.F.R. § 121.1 XIII(b)(1)(vi) (1996).

271 Defendant's Opposition to Plaintiff's Motion for a Preliminary Injunction at 1, *Bernstein v. United States Dep't of State*, 922 F. Supp. 1426 (N.D. Cal. 1996).

272 Chesapeake & Potomac Tel. Co. v. United States, 42 F.3d 181, 203 (4th. Cir. 1994) *vacated and remanded on other grounds*, 116 S.Ct. 1036 (1996).

273 *See* City Council v. Taxpayers for Vincent, 466 U.S. 789, 812 (1984).

the regulation is within the constitutional power does not warrant any deliberation.[274] The Arms Control Export Act (ACEA)[275] and the International Traffic in Arms Regulations (ITAR)[276] clearly establishes that the President has been delegated the authority under the law[277] and the Export Administration Act (EAA) establishes that the Secretary has authority under the law.[278]

Therefore, the ITAR regulations and EAA regulations that govern the export of encryption software, specifically source code, should be not be examined as governing "expressive conduct" based on the fact that the regulations do not meet three of the four prongs of the *O'Brien* test. As a result, source code should be analyzed as speech.

C. The Constitutionality of Regulating Source Code as Speech

Once it has been determined that source code is speech, the next analysis demands a determination whether the restriction is content-based or a time, place and manner restriction. A time, place or manner restriction may not have any reference to the content of the speech or stated by the courts is content neutral.[279] The standard for a time, place or manner restriction has been recognized by the court in *Community for Creative Non-Violence*, as being very similar in nature to the *O'Brien* test.[280] Therefore, based upon the earlier conclusions of the *O'Brien* tests, if the restrictions were found to be content neutral they would fail a time, place or manner test.

A content-based restriction relates to whether the application of the restriction turns on the substance or content of the speech.[281] The government regulation must be concerned with the communicative impact of the alleged "substantive evil."[282] In the *Karn, Bernstein* and *Junger*, the government's interest is focused upon the ability of the recipient of the encryption source code to alter plaintext to ciphertext. This governmental interest is clearly a content-based regulation. The Court has held that content-based restriction "will be upheld only if narrowly drawn to accomplish a compelling governmental interest."[283] Therefore, a regulation pertaining to a listener's or a reader's behavior from the communicative impact of the speech, receives a standard of review of the "most exacting scrutiny."[284]

A content-based restriction that is based upon a governmental licensing scheme is a form of prior restraint.[285] The ITAR regulations that govern the export of encryption software serves to prevent publication of encryption source code, which refers to a particular part of a computer language. The EAA also establishes a licensing scheme which restricts the export of items that do not meet particular requirements. The source code may be published when governmental approval is granted and a license is issued.[286] Governmental licensing comes with a heavy presumption against its constitutional validity.[287] The court established in *New York Times*, that the "disclosure . . . will surely result in direct, immediate, and irreparable damage to out Nation or its people."[288] A restriction of this type will not be upheld if based solely upon an "undifferentiated fear or apprehension of disturbance."[289] The measuring stick that all content prior restraint cases are evaluated against is whether the speech presents a danger equal to "publication of sailing dates of transports or

274 *See O'Brien* test, *supra* note 203.

275 22 U.S.C. § 2778 (1994).

276 22 C.F.R. § 120 (1996).

277 22 U.S.C. § 2778(a) (1) (1994).

278 50 U.S.C.S. § 2409(a)(1) (1996)

279 Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

280 Clark v. Community for Creative Non-Violence, 468 U.S. 288, 298 (1984) (noting that the *O'Brien* test differs little from the standard applied to time, place, or manner restrictions).

281 *United States v. Kokinda*, 497 U.S. 720, 754 (1990) (Brennan J., dissenting).

282 Schenck v. United States, 249 U.S. 47, 52 (1919).

283 United States v. Grace, 461 U.S. 171, 177 (1983).

284 Boos v. Barry, 485 U.S. 312, 321 (1988).

285 New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam).

286 The process that an encryption export application goes through is further support that the regulation is content-based. As each license application is reviewed by NSA and other relevant agencies, they review the "content of the software to determine whether it is harmless . . . or dangerous . . . and "the decision hinges entirely on what the reviewer concludes about the content of the speech." Appeal Brief of the Appellant at 31, Karn v. United States Dep't of State, *appeal docketed*, No. 96-5121 (D.C. Cir. Sep. 20, 1996).

287 Carroll v. President & Comm'rs of Town of Princess Anne, 393 U.S. 175, 181 (1968).

288 *New York Times*, 403 U.S. at 730 (Stewart J., concurring).

289 Cohen v. California, 403 U.S. 15, 23 (1971) (quoting Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503, 508 (1969)).

number and location of troops."[290]

The arguments advanced by the government in the *Karn* case suggest that the restriction is based only upon a speculative fear. The assertion that Mr. Karn's book "can be expected to result in far more actual use of encryption overseas, and thereby complicate even more the signals intelligence mission of the United States" is based on two assumptions.[291] The first assumption is that actual use of encryption overseas will not increase without the export of U.S. encryption products. As advanced earlier, the number of foreign readily available encryption software products have risen steadily and appear to be unaffected by the restrictions in the United States. The second assumption is that government's efforts will be further complicated by an increase in encryption use. As of late 1994, the FBI was unable to point to a single case where encryption had hampered an investigation.[292] The assumption is also based on the conclusion that the law enforcement's technology will not advance in step with the criminal technology. A former General Counsel for NSA recently acknowledged that there were few institutions other then the government that had the energy and resources to make efficient encryption software and products.[293] With the capabilities and resources of no other private institution, it is highly unlikely that the government's efforts will be complicated now or in the forseeable future.

Therefore, based on the fact that the government's rationale for the licensing of encryption software for export is founded purely on an undifferentiated fear, this form of prior restraint must be found unconstitutional.

VI. ONE POSSIBLE WAY TO DEAL WITH THE CRYPTO-GENIE

There is no denying the fact that the Crypto-genie is out of the bottle and flourishing throughout the world. The U.S. government's attempts, up to this point, have fallen short. A quasi-mandatory program implemented on the Internet, a worldwide network with no central interface, is doomed to a certain failure. But, by the same token, a completely unguided and unregulated encryption policy is just as short-sighted.

The interests of law enforcement are tantamount to the survival of any society. The potential for injury has only increased with the emergence and growth of computer technology. What was impossible to steal a few years ago, is now feasable with just a keystroke. Within a blink of an eye, a file cabinet worth of national security information is in the hands of an adversary. However, the effectiveness of law enforcement's efforts should not be based upon the yielding of one's individual rights. If law enforcement was not restrained to abide by one's personal rights, then practices such as warrantless searches and non-evidentiary hearings would be routine. This would undoubtedly bring about more "effective" law enforcement, but also at an enormous cost.

The solution must come in incremental stages to ensure success. The U.S. Government must realize that in order for any long term encryption policy to be successful, it must advance proposals that recognize the structure of the Internet. Attempts to govern the Internet through multinational agreements are inappropriate.[294] The Internet does not recognize borders or countries.

---

290 Near v. Minnesota, 283 U.S. 697, 716 (1931) (holding that the danger of war allows for limitations upon certain content of speech).

291 Reply Memorandum in Further Support of Defendants' Motion to Dismiss, or in the Alternative, for Summary Judgment at 6, Karn v. United States Dep't of State, 925 F. Supp. 1 (D.C. Cir. 1996).

292 Hoffman, *supra* note 6, at 5.1.

293 Stuart Baker, General Counsel of NSA, Remarks at the Fourth Annual Conference on Computers, Freedom and Privacy, session entitled "Data Encryption: Who Holds the Keys?" at the John Marshall Law School, Chicago (Mar. 24, 1994) (visited Jan. 25, 1997) <http://www.cpsr.org/dox/conferences/cfp94/encpanel.html/>.

294 Ineffective, as well as not in a particular country's best interest. A recent example in France serves as an ample warning. During the administration of Francois Mitterrand, over 1,500 people were illegally wiretapped. Yves LeRoux, Representative from French Office of Digital Equipment, Remarks at the Annual International Cryptography Institute Conference (Oct. 26, 1996). Some of the illegal wiretaps included Edqy Plenel, a journalist who broke the story that French agents were responsible for the bombing of the Greenpeace ship Rainbow Warrior in New Zealand in 1986. Another unsuspecting individual was Franois Froment-Meurice, the deputy leader of the opposition party. *See* Dave Banisar, *French Wiretapping Scandal Leads to Electorial Defeat*, (visited Oct. 20, 1996) <http://www.eff.org/pub/ . . . wiretap_scandal.article>.

Therefore, unless every country that has access to the Internet is able to agree upon the standards, the U.S. government must advocate a predominately domestic agenda with regards to controlling the ill effects of encryption.

The first stage is to establish a *truly voluntary* key escrow system with limited governmental involvement. The finite governmental involvement should be in the form of advocating the establishment of standards and nothing else. This open-ended program will allow for the encryption industry to explore a variety of different concepts and eventually produce encryption systems that will be compatible with any type of product. Undoubtedly, the business community will be more receptive to the products because of the unintrusive nature of governmental involvement and the ease of compatibility promises the least amount of lost revenue. As a result, as the business community embraces the open-ended encryption products, individuals within society will have no choice but to accept what the market has produced. This will also be extremely advantageous to the law enforcement community since it will not need to understand a number of different systems and products.

At first blush, this proposal may appear to be quite similar to the current initiative proposed by the White House. However, it is in fact, quite dissimilar. First, research and development would be conducted completely independent of governmental control. This would allow for industry to focus its efforts and precious resources on establishing a secure form of communication, instead of focusing on the development of a key recovery system that allows government to have access communications. Second, would be the sizable difference in the rate of penetration of encryption technology absent governmental involvement. Based in part on some of the aforementioned incidents involving governmental abuse, the general public is quite suspicious of programs that involve the government and "national security." Governmental involvement, through programs like key escrow or key recovery, as stated by the National Research Council, "[are] not appropriate at this time" and "[are] likely to have a significant impact on the natural development of applications."[295] Lastly, from a strictly policy perspective, advocating the control of society's technology when the capabilities of law enforcement are limited as a result of its growth is simply unwarranted. One of law enforcement's primary responsibilities is to keep up with the criminal element in our society, and this should not be achieved by expecting the rest of society to become technologically stagnant.

At this point, it is critical to emphasize that it is absolutely fundamental that law enforcement continues to use all of its available resources to neutralize criminal activities. These resources can come in the form of continued research and improvement of encryption capabilities or the improvement of other areas of intelligence methods. Long-range bugging devices, satellite imaging and relay devices are only a few of the devices that provide some of the same information, without the enormous costs upon one's individual rights.[296] It has also long been recognized that signal intelligence, who talks to whom, is in itself of significant value.[297] The capabilities of existing technologies, integrated services digital network (ISDN), provides information about who called whom, when and how long the communication took place.[298] Therefore, just as we should not be asked to use weaker locks on our doors, we should not be expected to use weaker encryption on our communications.

Stage two will comprise the development of a law enforcement structure to effectively combat criminal aspects of our society that utilize encryption but preserving the rights afforded by the First Amendment.

A possible remedy to the Crypto-genie is dealing with it in the same manner law enforcement currently deals with obtaining a warrant for a wiretap or searching one's house. In the case of an encrypted computer communication, the officer would obtain independent evidence that particular conversations between two parties were of a criminal nature. Upon court authorization, the

---

295 National Research Council, *Report on Cryptography's Role in Securing the Information Society*, (Pre-publication copy, Nat'l. Acad. Press 1996).

296 Michaël Johnson, *Data Encryption Software and Technical Data Controls in the United States of America* (visited Jan. 25, 1997) <http://www.eff.org/pub/Privacy/ITAR_export/us_crypto-policy.faq>.

297 Peter Coffee, *Privacy Defies Digital Designers*, PC WK., July 3, 1995, at 56.

298 *See generally*, The Administration's Clipper Chip Key Escrow Encryption Program: Hearings on S. J-103-55, Before the Subcomm. on Technology and the Law at 40, 103rd Cong., (1994) (statement of Dr. Whitfield).

officer would be granted permission to super encrypt or encrypt on top any messages between the two alleged parties. The super encryption would cause the message to be unreadable by the either party of the communication. Either party to the communication would then be given the opportunity to contest the seizure within a prescribed period of time. If the seizure is contested, the party to the communication would have to prove by a minimal standard that the communication was not of a criminal nature. The procedure could be done *in camera*, to protect any privacy concerns. Should the moving party be unable to meet his or her burden, the officer would be able to use any and all available means to decrypt the communication. This procedure would allow parties to communicate without the fear that any particular message could be intercepted and read without any notice and opportunity of a hearing.

Unfortunately, this recommendation does suffer from the inability of providing law enforcement with "real-time" access. However, the utilization of doors, locks and alarm systems have also contributed to law enforcement's inability to have "real-time" access, but we have not limited how society may utilize these devices to protect their rights. Further, to rely upon a certification system, as proposed by the government, demands that some degree of centralization to exist on the Internet, which will inevitably lead to abuse.[299]

This approach serves as a realistic solution to a problem that can never be totally controlled. New and innovative technology is developed everyday which will restructure this debate for many years to come. An example is a software product called Power One-Time Pad (POTP), which provides for encryption without the use of any keys.[300] It synchronizes random processes on two computers as they communicate. Each sequence of communication is encrypted with a different set of random processes. This system also removes any need for knowledge of another's keys. However, as stated a number of times before, this product like so many other new products because of its high key bit length, is in violation of export regulations and as a result this technology will be kept from the public. This products serve as only one example of how technology dictates the policy concerning cryptography. In conclusion, one can only hope that the debate will continually be guided by the words of Justice Brandeis who stated that, "[t]he right to be left alone — the most comprehensive of rights and the most valued by civilized men."[301]

---

299 *See* John Gilmore, *Clipper III Analysis* (visited Jan. 25, 1997) <http://www.crypto.com/eff.html>.

300 Winn Schwartau, *Network Security Without Keys*, NETWORK WORLD, Oct. 16, 1995, at 53.

301 Huguez v. United States, 406 F.2d 366, 374 n. 64 (9th Cir. 1968) (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). Ironically, in the *Olmstead* decision the Supreme Court held that wiretapping evidence did not need court authorization; I would like to extend my deepest gratitude to the Electronic Frontier Foundation, Ms. Cindy Cohn and Daniel Bernstein for affording me the opportunity to work along side them as part of the litigation team. The insight and knowledge that it afforded me allowed me to construct a more valuable work.