Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR and Their Successors[*]

TABLE OF CONTENTS

[*] B.A., University of Oregon Honors College; J.D. candidate, University of San Diego School of Law, 1998; M.A. International Relations candidate, University of San Diego College of Arts and Sciences, 1998. The author will be joining the Orange County office of Gibson, Dunn & Crutcher LLP as an associate in the Fall of 1998. Special thanks to my parents for their suggestions and endless barrage of articles related to this topic, to Heather for her cheerful willingness to listen to me sort through the issues raised in this Comment, and to Professor Larry Alexander for his insight into these issues. The author can be reached via e-mail at rmurr@usa.net.

I. INTRODUCTION

A. The Internet

A federal district court recently described the Internet as a "never-ending worldwide conversation."[1] The subject matters of this "conversation" are as diverse as one can imagine, with speakers' interests ranging from academia to anarchy. This new global forum permits people to converse, correspond, shop and conduct many other transactions conveniently over phone lines spanning neighborhoods and continents.[2] However, the increase in convenience with which these transactions can be conducted has also led to a decrease in privacy. Transactions and conversations that were once face-to-face and private are now taking place at a distance over computers and phone lines vulnerable to attack and eavesdropping from any computer-savvy technophile.

[1] ACLU v. Reno, 929 F. Supp. 824, 883 (E.D. Pa. 1996), *aff'd* 138 L. Ed. 2d 874, 1997 U.S. LEXIS 4037, 117 S. Ct. 2329. The Internet began in 1969 as computer network designed to link the military, military contractors and research universities together in the event of a war. From this, the current civilian form of the Internet evolved. ACLU v. Reno, 117 S. Ct. 2329, 2334. For more background information about the Internet, see generally ED KROL, THE WHOLE INTERNET (2d ed. 1994). Because of the nature of this topic, a number of the resources discussed in this comment were taken from Web pages on the Internet. These documents are available from the author and available on-line at the Universal Resource Locator (URL), or "address," indicated in the corresponding footnote. The brackets ("<" ">") enclosing the addresses are not a part of the URL.

[2] The Internet's most commonly used features are news groups, "chat rooms," the World Wide Web, and electronic mail ("e-mail"). These features permit users to receive and, in some cases, transmit, information of every possible kind. As of November 1996, there were an estimated 30 million Web pages on the Internet. Gary Rodan, *Information Technology and Political Control in Singapore*, Japan Policy Research Institute Working Paper No. 26, Nov. 1996, at 3 (on file with author). As of January 1997, an estimated 57 million people spread across 194 countries were connected to the Internet, and 71 million people were connected to e-mail servers. Rodger Doyle, *Access to the Internet*, SCI. AM., July 1997. A "server" is a central computer through which messages and commands are relayed to users at remote terminals. For information about the benefits of using e-mail over alternative forms of communication, see *infra* note 296. E-mail is one of the oldest and most popular uses of the Internet.

Security and privacy are special concerns on the Internet because messages, en route to their final destination, frequently pass through computer systems operated by private individuals, educational institutions, government agencies, or public interest organizations. Along the way, electronic messages can easily be intercepted, read, and even altered.[3] Moreover, with the increasing interconnectedness of computer systems, sensitive information like customer data, financial statements, research results, employment records, medical histories, and tax returns are vulnerable to attack, alteration or unauthorized disclosure.[4]

Many people dismiss these potential threats, believing themselves securely anonymous on computer networks. "Who would want to monitor my e-mail?" is a response frequently heard when unsuspecting computer users are warned of the lack of privacy on-line. Although electronic eavesdropping can certainly be targeted at a single person, it need not be. Technology exists that permits an eavesdropper to scan the contents of massive volumes of e-mail and other electronic data for preprogramed words or phrases.[5] A knowledgeable technician monitoring an Internet router could set up a search that makes copies of all

[3] Marcelo Halpern, *E-Mail Use in the Workplace: Avoiding the Pitfalls*, THE INTERNET NEWSLETTER: LEGAL AND BUS. ASPECTS, July, 1996, at 11. Despite the present deficiencies in privacy and security associated with the Internet, many attorneys (18% of those using the Internet) transmit confidential information via e-mail. Only 9% of attorneys using the Internet use some form of encryption to protect these confidential transmissions. INTERNET NEWSLETTER: LEGAL AND BUS. ASPECTS, July 1996, at 2.

These deficiencies led one observer to comment, "[t]he Internet, by its very nature, is not a good place to conduct business or send sensitive, confidential information. . . . A reasonable person wouldn't send sensitive information over the Internet." *Technical Tips: Getting Started Despite Security Scares*, COMMUNICATIONS WEEK, Sept. 9, 1996, at 63.

On protecting the privacy of files and databases from outside hackers, see generally D. BRENT CHAPMAN & ELIZABETH D. ZWICKY, BUILDING INTERNET FIREWALLS (1996).

[4] Ilene Rosenthal, *Export Controls on Mass Market Software With Encryption Capabilities*, THE THIRD CONFERENCE ON COMPUTERS, FREEDOM AND PRIVACY '93 PROGRAMS AND PAPERS, 6.25 (1993) (on file with author). The rise and predicted rise in telecommuting—working remotely from home—gives further cause for concern about the risks associated with transmitting sensitive data over computer, phone and fax lines.

[5] Three years ago, computer programmer and encryption advocate Philip Zimmerman warned that it was theoretically possible to set up computers to scan computer networks for certain words. He likened this to "driftnet fishing." Sandy Shore, *Controversy for Computer Privacy Code*, CHI. TRIB., Aug. 8, 1994, at Business 6. More recently, Wall Street investment firms have been able to use new software that can automatically monitor electronic correspondence between brokers and clients, scanning for evidence of securities violations. Joshua Quittner, *Invasion of Privacy*, TIME, Aug. 25, 1997, 28, 35. *See also infra* note 295.

messages passing through the router containing words of interest to the technician.[6] Because these "driftnet" search techniques allow searches by content, as well as by sender or receiver, the eavesdropper may intercept and read the messages of persons he has never even met.

The answer to these high-tech problems may lie in a very old process—using ciphers to make data and communications unintelligible to would-be eavesdroppers. Ciphers have been used for centuries, ranging in form from something as simple as a decoder ring to complex machines developed for use in warfare.[7] By encoding data and correspondence, senders and recipients can virtually assure themselves of privacy. Although many seek this assurance, not everyone agrees that ciphers ought to be more widely available.

Seeking to preserve its ability to wiretap domestic criminal suspects and eavesdrop on the secret communications of foreign governments,[8] the federal government has tried to prevent the proliferation of encrypting software—powerful ciphers generated by computers that allow users to protect their privacy through secret codes.[9] These

[6] It does not require much creativity to think of potential search terms that our fictitious technician might use. A "router" is a piece of computer hardware that directs the flow of traffic across computer networks. When messages are sent over the Internet, routers scan network connections and send the message through the portions of the network with the least congestion. As a result of the frequent detours that routers throw up, messages rarely travel a linear route from the sender to the recipient. Routers permit Internet traffic to move more quickly, but the sender of a message has no control over the path through which the message is sent.

[7] "One if by land and two if by sea" is an example of a cipher dating back to the Revolutionary War. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PENN. L. REV. 709, 713 (1995). For information concerning more recent uses of encryption by the military, see *infra* note 13.

[8] The government, as the defendant in one of the most significant cases in this area of law, stated that:

> [a] critical national security interest is to maintain an effective capability to gather foreign intelligence information. History is filled with examples of the need for the United States to break foreign codes in order to determine where enemy ships, submarines, and troops have been deployed, and other critical intelligence information. Through export restrictions, the United States seeks to control the foreign availability of cryptographic devices and software that might end up in the wrong hands, be deployed against the United States, hinder the government's foreign intelligence collection efforts, or otherwise undermine crucial national security interests.

Memorandum of Points and Authorities in Support of Defendant's Motion to Dismiss, or in the Alternative, for Summary Judgement, Karn v. United States Dep't of State, 925 F. Supp. 1 (1996) (visited Feb. 8, 1998) <http://people.qualcomm.com/karn/export/memorandum.html> [hereinafter Karn, *Points & Authorities*].

[9] These ciphers work by churning the message through a mathematical formula that creates garbled text as the output. This garbled message is transmitted and then descrambled by its recipient.

Here is an example of the scrambled output created by PGP, a popular encryption program. The original message was simple, "sample PGP output." The encrypted attempts to control encryption have taken the form of government-created encryption systems engineered to guarantee government access, and of controls on the export of privately created encrypting equipment and computer programs.[10]

This Comment discusses the need for privacy over the Internet and looks at the constitutional validity of previous and current regulations governing the export of privacy-enabling technologies. In particular, it seeks to analyze the constitutionality of the current regulatory scheme in light of the competing interests of privacy and freedom of expression on the one hand, and the need to protect national security on the other.

B. Encryption

The process of changing plain text into unintelligible code is called "encryption."[11] Changing an encrypted message back into plain text is

message reads:

```
——BEGIN PGP MESSAGE——
Version: PGP for Personal Privacy 5.0
MessageID: CNSaiNAgjCplO+vX0By79e9xFiR6ml8B
qANQR1DBwU4DOgd9PD+lHk8QB/0bBMW8cVqdmc2QxpDggGoSOv7fu
HiHXtyQXqneYls1dOhZ8XD99m8TUTO9S0M7fgcygX3S9WWPSlTtzBM2
WzNWH3VZhWDcULGxN7QChiGIM56bSbG1n9R10PMLEwT1FeFcZrt+
U9PmDWh3aXO5qZIEe86kNv8fMalklxdNnAqqridO4rMhYrA+OYrC+8k0
XoJqCeoK8Uce6q9bJzG2LuRN8g+z/M7IROdrLcZZ+VBOs1TESBfQ49X3t
NRkaavpea4eMehlM14DAO3u870BMIQhnTllXmKxFxUQbkpDz8dwVzlxm
nN91TJidhspJOu1NCi9n8sQMBiQ7x4vMYIK0T56CADVq6/Zxhz1VF8a2x
U+UPyFiGiWtECNHXbfFmm9WhJCEE6BSduJHjJrRTfsU/oDtBRNVsZO88
083ETzIrhDN/wlVU7yZzLQmmO6H7UHzC5nsHsCFwx7/1rvsQvU/wdAER
YAOiwo/QKtAdPf3tvrsL5fYi8vItwn3tFTNV5VitIk9EtuUD35ldZYbLQvb8D
OOPmLq0xvidLwPea6Df2QIQkOezFdZwAr6NaM8pk1GMG58PBPD8xZE
RZu1lCUd1wnEfiTU1PYrI21lHqKxJvonC/8KaVs+Qy0XmLi4JSBAWDrjsl
R844uiqHJyp4lhG6q27g–jJowKEGDhrpE5CoHrBvyTN1vBmsp+Xmzdq+0h
limvJ2IE3bC3fT6wr09yB3Of0X7J+IlfWUY0xN+7MGstGiDRMIGfQ==HRck
——END PGP MESSAGE——
```

As is apparent, this is a very sophisticated way of protecting the privacy of a message. The output, called "ciphertext," cannot easily be reduced to an intelligible message.

[10] Recently, the Clinton Administration has proposed domestic regulations that would establish a key escrow system for those wanting to participate in public key programs. *Administration Proposes Domestic Encryption Controls*, 3 CDT POLICY POST, Mar. 26, 1997 (copy on file with author and available on-line at (visited Feb. 8, 1998) <http://www.cdt.org/publications/pp_3.02html>).

[11] Encryption and digital signatures are closely related. For more information on digital signatures and proposed legislation that would create the necessary infrastructure to make the use of digital signatures economically feasible, see C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public*

called "decryption." In order to decrypt an encrypted message, one must have the code or "key" that corresponds to that message.[12] For years, encryption was the exclusive domain of the military intelligence community[13] and advanced mathematics classes.[14] However, recent advances in computer-generated encryption have brought this technology

Key Structure, 33 SAN DIEGO L. REV. 1143 (1996).

[12] Encrypting and decrypting codes are commonly referred to as "keys." For a discussion of the different types of keys currently in use, see generally BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 2-4 (1994). Modern encrypting systems use either one or two keys. The one key or "symmetric" systems work much like a traditional decoder ring. The sender and receiver must negotiate beforehand to share the secret key. Although effective, this system presents the problem of how to share the encrypting/decrypting key without compromising its security. Two key (asymmetric) crypto systems solve this problem. With the two key system, each user has a unique pair of keys: a "public key" and a "private key." To encrypt a document, the sender first looks up the receiver's public key, much as one would look up a phone number in a telephone directory. The message is then encrypted using the public key and is sent. Once the sender has encrypted the message with the public key, only the holder of the recipient's private key can decrypt the message. Describing the two key system, one author likened the technology to a voice mail system:

> With [a voice mail] system, you are assigned both a phone number (including a mailbox number) and a password. The phone number/mailbox number combination is public and may be given out to anyone you wish. People may then call in and leave you messages in your mailbox. However, since only you know your password, only you can gain access to your messages.

WAYNE M. GONYEA, SELLING ON THE INTERNET 27 (1995).

In addition to ensuring privacy, the two key system can also be used to verify the source of messages sent over the Internet. By encrypting a message twice, once with the recipient's public key, and again with the sender's private key, the recipient can verify the identity of the sender. This double encryption process allows the recipient to rest assured that no one else can read the message he has been sent and, by successfully decrypting the message with the sender's public key, he can be certain of that the message is authentic.

As a general rule, the longer the key, the harder it will be for an eavesdropper to unscramble the message. This basic concept is central to the discussion in this Comment and the debate surrounding the regulation of encryption. The government regulations are triggered by the length of the key. Because of the mathematics involved, key lengths of an asymmetric/public key system and a symmetric/private key system cannot be compared on an apples-to-apples basis. For example, a 40-bit symmetric key offers approximately the same degree of protection as a 512-bit asymmetric key. For ease of discussion, key lengths mentioned in this paper refer to symmetric systems, unless otherwise noted.

[13] For information on military applications of encryption technology during WWII, see generally THE CODE BREAKERS (F. H. Hinsley & Alan Stripp eds., 1993); Doris A. Paul, THE NAVAJO CODE TALKERS (1973).

[14] Computer generated codes are driven by mathematical algorithms. Thus encryption is occasionally a subject dealt with in advanced college level mathematics courses. In fact, cryptography has been described as "fundamentally based on problems that are difficult to solve." Paul Fahn, *Answers to Frequently Asked Questions About Today's Cryptography*, (published by RSA Laboratories) at 12 (visited Oct. 5 1996) <http://www.rsa.com/rsalabs/newfaq/home.html> [hereinafter Fahn, *FAQ*]. An "algorithm" is a mathematical term, defined as a "step-by-step problem-solving procedure." AMERICAN HERITAGE DICTIONARY (3d ed. 1992).

to the private sector, making it possible for ordinary citizens to communicate in codes so secure that not even the United States military can decipher the encoded messages.[15] These strong encrypting algorithms, which derive their strength from the length of the key,[16] are sometimes called "military-grade" encryption.

Today's military-grade encryption uses long combinations of numbers and letters to ensure the privacy of the encrypted message. Even slight increases in key length yield exponentially more secure ciphertext. A 64-bit key (symmetric) is 256 times more difficult to crack than a 56-bit key. Cracking a 128-bit key[17] would require the use of all 200 million computers estimated to exist in the world and would take one million times the age of the universe to exhaust all possible key combinations.[18] In contrast, it was estimated in 1996 that any individual could crack a 40 bit key such as "apple" in 12.7 days with the use of a single

[15] *See infra* notes 18-20 and accompanying text.

[16] Encryption security depends on the length of the key, measured in "bits." Two key (asymmetric) systems require significantly longer keys to ensure the same level of privacy as a shorter one key (symmetric) system. All keys referred to in this Comment 128 bits or shorter are symmetric keys; anything over 128 bits is an asymmetric key.

[17] A symmetric key 128 bits long has 1.0 x 10^{37} possible key combinations generated from a password of just 16 characters. A 40-bit key, corresponding to a password only five characters long, such as "apple," produces a mere 932 billion (9.32 x 10^{11}) key combinations. David Friedman, *A World of Strong Privacy: Promises and Perils of Encryption*, 13 SOC. PHIL. & POL'Y J. 212, 214 n.5 (1996); *see infra* note 19.

[18] SCHNEIER, *supra* note 12, at 136. Note that these estimates denote the amount of time required to check all possible key combinations. Cracking a code by checking all the possible combinations is called a "brute force attack" and may not be the most efficient way of breaking a code. It is possible that an eavesdropper will get lucky on her first try and stumble across the key. However, the chances of this happening are virtually nonexistent. Statistically speaking, the key will usually be found mid-way through the process. This means that, on average, it will take only 500,000 times the age of the universe to crack a 128-bit key. *Id.*

Cryptographers have recently discovered a new way to crack even the strongest codes used in encrypted "smart cards." This method relies not on computing power, but rather on a phenomenon that occurs when smart cards are irradiated with microwaves. John Markoff, *2 Israelis Outline New Risk To Electronic Data Security*, N.Y. TIMES, Oct. 19, 1996, at A38.

Finally, researchers at IBM recently announced that they may have developed a new encryption scheme that is completely unbreakable. Although practical applications of the newly discovered mathematical problem are some time off, such a development would be significant for privacy advocates, criminals and law enforcement officials. Ed Golden, *IBM Encryption Scheme Holds Significant Promise*, INFOWORLD, May 21, 1997, at 21.

personal computer.[19] By using 100 computers collaborating to break the code, the time needed is reduced to three hours.[20] Journalists have reported that the American government can crack a 56-bit symmetric key in fewer than 12 seconds.[21] Currently, a 40-bit symmetric key is the longest key exportable from the United States for general use abroad without obtaining any permission from the government.[22] The Commerce Department will grant a license to export encryption with key lengths up to 56 bits if the exporter agrees to implement a key recovery system that will be operable within two years.[23] Key length alone is the measure by which administrative agencies initially decide whether to scrutinize the export of certain encryption technology.

Although today's most secure keys appear dauntingly long, rapid developments in computer processor speed may make these encrypting algorithms vulnerable to attack.[24] Such has been the fate of the most

[19] Friedman, *supra* note 17, at 214. Although a 40-bit key is considered relatively weak, using the keys found on a standard computer keyboard yields roughly 9.32×10^{11} (932 billion) possible key combinations even with this "weak" key. Making the same assumptions about the keyboard characters available for use, a 56-bit key has 5.52×10^{17} possible key combinations (where 56 bits corresponds to a 7-character key; 7! = 5040; and the keyboard has 95 characters. Thus, $1/5040 \times (1/95)^7 = 2.83 \times 10^{-18}$. The odds of guessing the right key are consequently, 1 in 5.52×10^{17} possible key combinations).

[20] SCHNEIER, *supra* note 12, at 260.

[21] Kristi Essick & Jeff Algh, *Encryption Policy Fails to Please U.S. Vendors*, 18 INFO WORLD, Oct. 7, 1996, at 14.

[22] *Encryption Items Transferred from the U.S. Munitions List to the Commerce Control List*, 61 Fed. Reg. 68572 (1996) (action interim rule Dec. 30, 1996) codified at 15 C.F.R. §§ 700-99 (1997) [hereinafter Interim Rule]. Until recently, exporting any encryption using a key longer than 40 bits required registration with the State Department as an arms dealer. Paul Fahn, *RSA Frequently Asked Questions About Cryptography Export Laws* at 4, 10 (published by RSA Data Security) (visited Feb. 8, 1998) <http://www.rsa.com/PUBS/exp_faq.pdf> [hereinafter Fahn, *Export FAQ*].

[23] Interim Rule, *supra* note 22. The Department of Commerce will review these licenses every six months to ensure that progress benchmarks are met. *Id.* at 68574. A "key recovery system" is a mechanism that permits law enforcement officials seeking to eavesdrop on a suspect to retrieve an encryption key from a key-escrow agent.

[24] Gordon Moore, co-founder of Intel Corporation, observed that computer processor manufacturers could double the speed of their processors every 18-24 months. For nearly 40 years, Moore's observation, dubbed "Moore's Law," has proven accurate. Nevertheless, Moore and other industry experts doubt whether this rate of change can continue much longer. Gordon E. Moore, *Can Moore's Law Continue Indefinitely?*, COMPUTERWORLD, July 1, 1996, *available in* LEXIS, NEWS Library, PAPERS File; *see also* G. Dan Hutcheson & Jerry D. Hutcheson, *Technology and Economics in the Semiconductor Industry*, SCI. AM., Jan. 1996, at 54.

The Economist recently reported that the Defense Advanced Research Projects Agency (DARPA) is investigating the possibility of creating a quantum computer, a machine theoretically capable of simultaneously contemplating 125 alternative solutions to a problem. Today's computers can contemplate only one solution at a time. The new machine might be capable of cracking codes that are uncrackable with present technology. *The Weirdest Computer of All*, ECONOMIST, Sept. 28, 1996, at 97-98.

widely used encryption system in the world today, the Data Encryption Standard (DES). In 1977, engineers at IBM working with the United States government developed DES. Operating on a 56-bit symmetric key, DES has since become the most widely used encryption system in the world today, and yet only recently has one been allowed to export it without first registering as an arms dealer.[25]

Although DES appears to remain relatively safe,[26] experts agree that a newer encryption standard with a longer key should be used in the future.[27] The National Institute on Science and Technology (NIST) has recertified DES as the official encryption standard of the United States government every five years since its creation in 1977.[28] DES was last recertified in 1993.[29] NIST has indicated that it may not re-certify DES in 1998, however.[30]

As computer networks become more interconnected and people increasingly use electronic media to store and transmit sensitive information, demand for encrypting software has increased greatly.[31] At the same time, computers have become faster, making encryption that was once secure vulnerable to attacks by those armed with the latest machinery. As a result, both real and imagined vulnerabilities in today's encryption have increased the demand for stronger encrypting hardware and software.[32]

In response to this demand, and in an effort to frustrate governmental efforts to stem encryption proliferation, a computer programmer named Phil Zimmerman privately distributed a military-grade encryption

[25] Under the old encryption regulations, one had to first register as an arms dealer before permission to export could be granted. Under the new standards, one must now commit to producing a key recovery system within two years, surrender the decryption keys on export, or export only weak encryption. *See infra* Part II.B.

[26] In 1994, an attack could be successfully performed on a DES key in 3.5 hours but required an estimated one million dollars worth of equipment. Fahn, *FAQ*, *supra* note 14, at 70.

[27] Scientists at RSA currently recommend key lengths of at least 80 bits symmetric and 768 bits asymmetric. Fahn, *Export FAQ*, supra note 22, at 4.

[28] Froomkin, *supra* note 7, at 736 n.106.

[29] Revision of Federal Information Processing Standard (FIPS) 46-1 Data Encryption Standard (DES), 58 Fed. Reg. 69347, 69347-48 (1993).

[30] Fahn, *FAQ*, *supra* note 14, at 70.

[31] Rosenthal, *supra* note 4, at 6.25.

[32] *Id.*

program that quickly made its way onto the Internet.[33] Since Zimmerman made available copies of his program "Pretty Good Privacy" (PGP) in 1991,[34] copies of the program have spread to all four corners of the globe, much to the chagrin of law enforcement agencies worldwide.[35] After news of the international proliferation of PGP spread, the United States Customs Service launched an investigation of Zimmerman that lasted three years. The Customs Service closed the investigation in January 1996 without an indictment.[36] PGP, operating with asymmetric key lengths from 512 to 4096 bits, is virtually unbreakable.[37]

[33] A copy of PGP, Zimmerman's program, can be downloaded for free from the MIT server. (visited Feb. 8, 1998) <http://web.mit.edu/network/pgp>.

[34] The United States Customs service investigated Zimmerman for three years in connection with the posting of PGP and its subsequent distribution abroad. The investigation was closed in January, 1996 without an indictment. Phil Zimmerman, *Verbatim*, COMPUTERWORLD, July 22, 1996, at 37.

[35] Criminals have already started to use PGP to thwart criminal investigations. Pedophiles and neo-Nazis have used their computers to encrypt data that law enforcement officers suspect contain names of associates and contacts. Efforts to decrypt these files have proven futile. Eric Dexheimer, *Police Uneasy With This Cure for the Common Cold*, SAN DIEGO UNION TRIB. COMPULINK, Mar. 1, 1996, at 1. Within days of the supposedly restricted release of version 2.6 of PGP in the United States, a researcher in Hamburg Germany received a copy of the program. He subsequently made the program available on the University of Hamburg computer server. *See* Froomkin, *supra* note 7, at 750 n.167-68 and accompanying text.

"The International PGP Home Page," located on a server in Norway, offers information on PGP and links to servers offering PGP outside of the United States. It is located on the Web at (visited Feb. 8, 1998) <http://www.pgpi.com>. The purpose of the Home Page is "to promote the use of PGP worldwide, and to be a resource pool for information on PGP" (last modified Jan. 9, 1998) <http://www.pgpi.com/about>. This page provides links to computers offering the newest version of PGP (5.0 Windows 95) in Russia, Romania, Hong Kong, Indonesia, Brazil, Japan, Italy, Germany, Austria, Norway, the United Kingdom, Denmark, Sweden, Portugal, Spain, the Czech Republic, Finland, the Netherlands, Greece, South Africa, Hungary, Switzerland, and Australia (visited Feb. 8, 1998) <http://www.pgpi.com/download/> (from this page, select which version of PGP you wish to download and then click 'More Sites' to see the list of nations offering the program).

A British Web site lists servers throughout Europe which offer PGP for download (visited Oct. 5, 1996) <http://thegate.gamers.org/~tony/pgp.html>. The site cautions in jest, "Remember: Do not obtain PGP from a site in the USA or Canada, unless you are physically within the borders of the USA or Canada. Disobeying the above instruction is probably very very naughty." Although warning in jest, the author makes a good point. Downloading PGP from a computer located inside the United States or Canada to a computer outside of those nations violates EAR/ITAR export laws. However, downloading the same program from a computer outside of the United States or Canada is perfectly legal.

[36] Zimmerman, *supra* note 34, at 37.

[37] For a more complete treatment of PGP's specifications, refer to the PGP 5.0 Manual. (Note, because the manual contains information about PGP, it too is subject to encryption distribution limitations. A copy can be obtained with the PGP download after verifying that the user is connected through a computer server located in the United States. Alternatively, a copy is available from the author).

Members of the law enforcement community execrate this high level of security, much lauded by users of the Internet. Law enforcement officials at the local, state and national levels have lobbied for restrictions on the use and export of encryption in an effort to preserve their ability to eavesdrop on electronic communications.[38]

The release of PGP in 1991 has since fueled the debate over the right to privacy versus law enforcement's need to eavesdrop on criminal suspects.[39] In response to these concerns, and in an effort to stem the use of encryption by terrorists, members of organized crime, and drug dealers, the Clinton Administration in 1993 proposed a "key escrow system" popularly known as the "Clipper Chip."[40]

Initial public response to the Clipper Chip proposal was overwhelmingly negative.[41] Civil libertarians and industry representatives vociferously lobbied Congress to defeat the proposed legislation.[42] In

[38] FBI Director Louis Freeh testified in the last Congress against a Senate bill that would liberalize encryption controls. He argued that private encryption systems "can prevent police officers on a daily basis from conducting basic searches and seizures of computers and files . . . . Without the ability to promptly decrypt encrypted criminal or terrorist communications and computer files, we in law enforcement will not be able to effectively investigate or prosecute society's most dangerous felons." Ramon G. MacLeod, *Computer Privacy Could be Casualty of War on Terrorism-Government Wants Keys to Codes*, S.F. CHRON., Aug. 21, 1996, at A5.

[39] *See, e.g.*, John Mintz & John Schwartz, *Chipping Away at Privacy? Encryption Device Widens Debate Over Rights of U.S. to Eavesdrop*, WASH. POST, May 30, 1993, at H1.

[40] Essentially, the Clipper Chip system would work as follows: computer and communications equipment manufacturers would produce hardware that would encrypt and decrypt using "Skipjack," a classified encrypting algorithm developed by the National Security Agency (NSA) with a key length of 80 bits. The government would then hold a copy of the key used to decrypt communications scrambled with Skipjack. To appease consumers and civil libertarians, President Clinton proposed that the government-held key be split in two and stored with two "trusted escrow agencies." Froomkin, *supra* note 7, at 759. Both halves of the key would be needed to decrypt a scrambled message. Suggestions for escrow agencies have included the Treasury Department and the National Institute of Weights and Measures. To obtain the keys to decode a conversation or data transmission, a law enforcement agency would simply have to present a request to the escrow agency for the keys. For more information about the Clinton key escrow proposal, see generally Froomkin, *supra* note 7, at 742-64.

[41] "[N]early all of the comments received from [the US computer] industry [in response to the proposed standard] opposed the adoption of the standard." Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997, 5998 (1994) [hereinafter FIPS 185]; *see also* Kevin Power, *Industry Says No to Clipper*, 14 GOV'T COMPUTER NEWS, Aug. 21, 1995, at 73.

[42] Among the groups who lobbied against Clipper were: the ACLU, Microsoft, IBM, Apple Computer, Novell, and Sun Microsystems.

the wake of the negative publicity surrounding the Clipper Chip proposal, President Clinton dropped his plan for the development of a single national encryption standard developed by the government.[43] However, President Clinton continued to prohibit the export of hardware and software using strong encrypting algorithms. More recently, President Clinton has used the export control issue as a bargaining chip with a new encryption policy proposal, dubbed Clipper III.[44] The proposal "allows for the use of any method of encryption as long as the user stores an electronic key with a bank or other trusted third party [from whom the government can gain access to the key in connection with a criminal investigation]."[45]

The Clinton Administration has thus launched a two-pronged attack on the spread of strong encryption.[46] First, President Clinton has tried to regulate domestic use through proposed key escrow systems and the FIPS 185.[47] Second, President Clinton has tried to check the spread of privacy-enabling technology by applying export regulations to the export of cryptography, in order to reduce international availability. The second prong has slowed the proliferation of strong encryption both abroad and domestically. A recent report by a government commission created to study encryption policy issues noted the following:

> Export controls also have had the effect of reducing the *domestic availability* of products with strong encryption capabilities. The need for U.S. vendors (especially software vendors) to market their products to an international audience leads many of them to weaken the encryption capabilities of products

[43] In 1994, the government officially accepted the Escrow Encryption Standard (EES) for federal agencies as a voluntary standard. FIPS 185, *supra* note 41. Acting on this standard, the Department of Justice purchased 9,000 AT&T Clipper telephones using this technology. Froomkin, *supra* note 7, at 769. Although the EES is voluntary, it is the only standard approved by the government for government use. As a result, the EES is becoming a defacto national standard for federal agencies and those who wish to communicate securely with these agencies.

[44] Bruce W. McConnell & Edward J. Appel, *Enabling Privacy, Commerce, Security & Public Safety in the Global Information Infrastructure*, EXECUTIVE OFF. OF THE PRESIDENT, OFF. OF MGMT. & BUDGET (May 20, 1996) <http://www.cdt.org/crypto/clipper_III/clipper_III_ draft.html>. For more information about the original Clipper Chip proposals as well as the amended proposals, see generally (visited Feb. 8, 1998) <http://www.cdt.org/crypto/>.

[45] Michael Kantor, *Encryption Policy Balances Economic, Safety Concerns*, SEATTLE TIMES, Sept. 18, 1996, at B5; *see also* Ramon C. McLeod, *Computer Privacy Could be Casualty of War on Terrorism—Government Wants Keys to Codes*, S.F. CHRON., Aug. 21, 1996, at A5.

[46] "The government's response to [proliferation of encryption] has been twofold: an attempt to make the nation's phone and communication networks more open to government taps, and a drive to limit the spread of data encryption. . . . The government hopes Clipper will replace [private] chips providing unbreakable encryption for conversations." Mintz, *supra* note 39.

[47] *See supra* note 41.

> available to the domestic market. Thus, domestic users face a more limited range of options for strong encryption than they would in the absence of export controls.[48]

As communication and commerce become increasingly globalized, and as the American domination of high technology fields like cryptography wanes, the need for a single universal encryption standard increases.[49] Export regulations have had the effect of inhibiting the emergence of this universal encryption standard. The following Part looks at two generations of encryption regulations and cases challenging the regulations.

II. RESTRAINTS ON EXPORTATION

On November 15, 1996, President Clinton signed Executive Order 13,026, entitled Administration of Export Controls on Encryption Products.[50] This order, drafted in response to public demands for more liberal encryption export controls, changed the basic regulatory framework that had governed encryption exports since 1977.[51] Prior to this change, encryption technologies had been treated as "munitions" for purposes of export licensing. The State Department regulated these exports through a complex procedure that required the applicant to disclose details about the nature of the encryption, its intended and

[48] CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (Kenneth W. Dam & Herbert S. Lin eds. 1996). (Report by government commission comprised of the Committee to Study National Cryptography Policy, the Computer Science & Telecommunications Board, the Commission on Physical Sciences, Mathematics, and Applications, and the National Research Council) available on-line at <http://www.nap.edu/reading/reader.cgi?auth=free&label=uk.book.0309054753> (emphasis added) [hereinafter Committee Recommendations]; *see also* Friedman, *supra* note 17, at 224.

[49] "Such single products were subject to export control and thus the NSA acquired substantial influence not only over what was exported, but what was sold in the U.S." SCHNEIER, *supra* note 12, at xiii.

[50] Executive Order 13,026 Administration of Export Controls on Encryption Products (32 Weekly Comp. Pres. Doc. 2399, Nov. 15, 1996) [hereinafter Clinton Order].

[51] *Id.* Executive Order 11,958, 42 Fed. Reg. 4311 (1977) was the initial Presidential delegation of control over munitions exports under the authority granted to the Executive Branch by Congress in the Arms Export Control Act of 1977 (AECA), 22 U.S.C. § 2778. The predecessor to the AECA was the Mutual Security Act of 1954, formerly 22 U.S.C. § 1934. The President also delegated the power granted under the '54 Security Act to regulate encryption exports to the Secretary of State, Executive Order 10,973 § 105, 26 Fed. Reg. 10469 (1961).

potential applications, and its intended foreign recipient. President Clinton's Executive Order shifted regulatory responsibility for most commercial encryption to the Commerce Department. This move was ostensibly intended to liberalize the export controls and to encourage freer use of encryption. Although the new regulations are in fact more liberal than the previous ones, the underlying features of the two regimes are the same.

The salient features are these: both regulatory schemes require governmental approval prior to export; approval is tied to the security of the encryption, as indicated by the key length; and neither system purports to allow judicial review of decisions denying applicants permission to export their information.

The following Part discusses why the features shared by the new and old regulatory schemes are at the heart of the legal debate surrounding their constitutionality. In the end, it does not matter which arm of the Executive Branch regulates encryption. So long as a scheme exists which conditions permission to export of source code[52] on prior approval based on the strength of the encryption, and fails to permit judicial review of licensing decisions, the First Amendment is implicated. Thus, although President Clinton's shift of control from one regulatory body to another represents an historic change in regulatory policy, it represents little change in terms of the constitutional merits of the regulatory scheme. Because the Department of Commerce controls are so new, courts are just now considering the constitutional validity of the new regulations. In light of the underlying similarities between the old and new regulations, however, older cases and analysis considering the merits of the State Department regulations are on point.

The relatively recent district court decisions discussing the constitutionality of the old regulations under the Department of State are useful in determining whether the new Department of Commerce regulations and their successors are constitutionally permissible. The new Commerce Department regulations are governed by the Export Administration

[52] Source code is a precursor to software. By processing source code with a translation program called a compiler, the source code can easily be converted into object code, the actual binary language of computers. Software is a package that contains compiled object code. The debate surrounding encryption extends to both source code and software. For all practical purposes, there is no meaningful distinction between the two in the context of this debate. The following is an example of source code for part of a popular encryption program:

```
#!/bin/perlspo777i<X+d*1MLa^*1N%0]dsXx1M1N/dsMO<
j]dsj$/=unpack('H*',$_);$_='echo16dio\U$k"SK$/
SM$n\EsN0p[1N*11K[d2%Sa2/d0$^Ixp'|dc';s/\w//g;$_=pack('H*',/((..)*)$/)
```

(visited April 2, 1997) <http://online.offshore.com.ai/arms-trafficker/>.

Regulations (EAR).[53] The Department of State regulations were governed by the International Trade in Arms Regulations (ITAR).[54] When referring to encryption export regulations generally, I will use the combined acronym EAR/ITAR.

A. ITAR

With the passage of the Arms Export Control Act (AECA), Congress delegated to the President the authority to control the import and export of certain defense items.[55] The AECA grants the President the authority to create a list of items that are subject to import and export restrictions. This list is known as the "United States Munitions List" (USML).[56] The Secretary of State, acting under the authority of an executive order,[57] promulgated the USML as a part of the International Trade in Arms Regulations (ITAR).[58] As one might expect, the USML controls the export of weapons such as tanks, missiles, and other instruments of war. In addition, the USML controlled the export of encrypting devices, source code,[59] and software.[60]

[53] 15 C.F.R. §§ 730-774 (1997).

[54] 22 C.F.R. §§ 120-130 (1997).

[55] 22 U.S.C. § 2751-2799 (1994). These statutes include the provision that:

> In furtherance of world peace and the security and foreign policy of the United States, the President is authorized to control the import and export of defense articles and defense services. The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the United States Munitions List.

22 U.S.C. § 2778

[56] *Id.*

[57] Exec. Order No.11,958, as amended in 42 Fed. Reg. 4311 (Jan. 18, 1977).

[58] 22 C.F.R. §§ 120-130 (1997).

[59] Source code is "merely a means of instructing a computer to perform a function." Karn v. United States Dep't of State, 925 F. Supp. 1, 27 n.19 (D.D.C. 1996). *See supra* note 52.

[60] 22 C.F.R. § 121.1 (Category XIII) (1995). While dual use encrypting technologies were still under the control of the ITAR, the State Department classified as a munition a $300 device to be installed on top of a television set for browsing the World Wide Web and sending e-mail messages. The device, using a 128-bit cipher, is currently sold in stores such as Sears and Circuit City but could not be exported without an arms dealer license. John Markoff, *U.S. Classifies a Device to Surf the Web a Weapon*, N.Y. TIMES, Nov. 8, 1996, at D2. It is not clear whether this device is exportable under the newly modified EAR.

Under the ITAR regime, the Department of State determined whether an item is within the scope of the USML when the would-be exporter filed a Commodity Jurisdiction Request (CJR). If the Department of State found the item to be within the scope of the USML, that item could not be exported without a license.[61] The Office of Defense Trade Controls, Bureau of Political-Military Affairs, decided whether to grant or refuse a license for the export of an item that the State Department determined to be within the ambit of the USML.[62] A determination by the State Department that an item is on the USML meant that exporters and manufacturers of that item must register with the government as arms dealers or manufacturers.[63]

B. *Current Regulatory Framework: EAR*

Pursuant to the Export Administration Act of 1979[64] (EAA), President Carter issued an Executive Order delegating control over most of the EAA to the Secretary of Commerce.[65] After the delegation, the Department of Commerce promulgated the Export Administration Regulations (EAR).[66] Although the EAR did not originally have jurisdiction over the export of encrypting applications, it gained jurisdiction in 1996 with the issuance of the Executive Order 13,026.[67] By this order, the President transferred the regulation of all dual-use and nonmilitary encryption commodities, software, technology (both encryption hardware and software) and source code to the Commerce Department under the EAR effective December 30, 1996.[68] After this transfer, military encryption is still subject to regulation under the ITAR, while nonmilitary applications are now governed by the EAR.[69]

Although the EAR is certainly more liberal than the ITAR in terms of permitting the export of a variety of commodities without preapproval, certain EAR commodities still require a license before they can be

[61] 22 U.S.C. § 2778(b)(2) (1994).

[62] 22 C.F.R. § 120.1(a) (1997). Requirements for export licenses are set out in Part 123 of the ITAR. 22 C.F.R. §§ 123.1-123.26 (1997).

[63] 22 C.F.R. §§ 120.4, 122.1 (1997).

[64] The EAA is codified at 50 U.S.C.A. §§ 2401-20 (West 1991 Supp. 1997).

[65] Exec. Order No. 12,214, 45 Fed. Reg. 29783 (1980).

[66] "EAR" refers generally to 15 C.F.R. chapter VII, sub-chapter C. 15 C.F.R. § 730.1 (1997).

[67] *See* Clinton Order, *supra* note 50.

[68] *Id.*

[69] The rules governing this handover of control state that encryption that has been "specifically designed, developed, configured, adapted or modified for military applications (including command, control and intelligence applications)" will remain under ITAR jurisdiction. 61 Fed. Reg. 68633 (December 30, 1996). The rules governing non-military encryption can be found at 15 C.F.R. § 742.15.

legally exported.[70] These commodities are listed on the Commerce Control List (CCL), and include, among other things, certain encrypting applications and source code.[71] Depending on the strength of the encryption, the Commerce Department can grant a license for export, waive the requirement that the exporter file for a license, grant the license if the exporter agrees to create a key recovery system over the next two years, grant the license if the exporter hands over the keys to the encryption at the time of export, or deny the application.[72] Applications for export licenses are submitted to the Department of Commerce's Bureau of Export Administration (BXA).[73] Determinations whether to grant a license are made on a case-by-case basis.[74]

As of this writing, the Department of Commerce has promulgated an interim rule to govern what can and cannot be exported under the EAR.[75] These rules purport to liberalize controls restricting the export of strong encryption while taking the first steps toward creating a

[70] 15 C.F.R. § 730.7 (1997). "Export" is defined under the EAR as "an actual shipment, transfer, or transmission out of the United States . . . ; or [a] transfer of such software in the United States to an embassy or affiliate of a foreign country." 15 C.F.R. § 734.2(b)(9)(i)(A)-(B) (1997). In addition to shipping or transmitting encryption outside of the United States, the Commerce Department interprets the EAR's definition of "export" as it relates to encryption on the CCL to include the, "downloading or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo-optical, photoelectric, or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites, unless the person making software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States. . . ." 15 C.F.R. § 734.2(b)(9)(ii) (1997).

[71] The CCL control policies are found at 15 C.F.R. §§ 742.1-.15. The actual CCL is codified at 15 C.F.R. § 774. Encryption export controls are codified at 15 C.F.R. § 742.15 and listed on the CCL in Supplement No. 2 to Part 774.

[72] The rules dictating the exportability of certain encryption are rather byzantine. They can be reviewed by the bold at 15 C.F.R. §§ 742.15, 774.

[73] 15 C.F.R. §§ 730.7, 774.1 (1997).

[74] Letter from James A. Lewis, Director of the Department's Office of Strategic Trade and Foreign Policy Controls, to petitioner Peter Junger, dated January 29, 1997 (visited Sept. 1, 1997) <http://samsara.law.cwru.edu/comp_law/crypto_export/>. Petitioner Peter Junger's case against the government is discussed *infra* note 112.

[75] The Department of Commerce has not provided an estimate for when a final rule will be issued. *Semiannual Agenda of Regulations*, 62 Fed. Reg. 21520, 21541 (1997) (providing the date 00/00/00 on the timetable listing when the final rule corresponding to the Interim Rule will be promulgated).

"worldwide key management infrastructure."[76] While this key management infrastructure is being conceived, planned and created, the current regulations permit the export and re-export of up to 56-bit encryption, provided that the exporter promises implement a key recovery scheme over the next two years. The key recovery system envisioned in the Commerce Department's rules would permit law enforcement officials to crack the codes generated with the software that was exported under the rules. By requiring that exporters promise to implement such a system, the progress of which is measured every six months through the use of benchmark measures, the Department of Commerce has set up a goverment-initiated market-led conversion to a new key escrow system. Whether this system will enjoy any uniformity or general acceptance remains to be seen.

C. Common Threads in EAR, ITAR, and Future Regulatory Schemes

As previously explained, the EAR and ITAR regimes are nearly identical at their core. The central features of both are discussed below. Because of the salience of the regulated technology to law enforcement officials, corporations, and privacy advocates, changes to the form and the details of the EAR regime are certain to be ongoing. Nevertheless, so long as these core features remain a part of any regulatory effort that controls the export of encryption, constitutional concerns are raised.

1. Pre-Export Review

Both EAR and ITAR require that the would-be exporter obtain permission before sending the encryption out of the country. This is a logical requirement where the government has an interest in keeping secret information inside the country. However, any review prior to publication or distribution raises unique constitutional concerns discussed in the next Part.[77]

2. Strength-Based Determinations

Rather than impose a flat ban on all encryption exports or all exports to certain nations, both EAR and ITAR regulate encryption on the basis of the level of protection that it offers. Under the ITAR scheme, the Department of State granted permission to export encryption operating

[76] Interim Rule, *supra* note 22, at 68573. It is doubtful whether such an international scheme would ever be viable. *See supra* note 18.

[77] See *infra* Part III.B.

at a key length up to 40 bits. Encryption operating above the 40-bit threshold that could be used to encode a message[78] was rarely, if ever, allowed out of the country through legal channels. The Commerce Department has liberalized export rules by permitting the export of encryption with key lengths of up to 56 bits if the exporter promises to implement a key recovery system over the next two years that will ensure continuing law enforcement access to data and information encrypted with these algorithms.[79] Encrypting applications using keys longer than 56 bits cannot be exported without the immediate surrender of the keys.

Although the ITAR and the EAR differ in their treatment of encryption with keys lengths between 40 and 56 bits, both use the relative strength of the encryption to make distinctions between those programs that may be exported and those that may not. This inquiry into strength has constitutional implications as well.

3. *Judicial Review Not Permitted*

The presence of a right to judicial review is a necessary, though not sufficient, condition for a censorship scheme to pass constitutional muster.[80] To the extent that encryption licensing schemes can be likened to censorship schemes, the right to judicial review will be an important consideration in determining whether such a scheme is constitutional. The ITAR regulatory scheme does not permit judicial review under the generally applicable Administrative Procedures Act (APA).[81] Likewise, Clinton's executive order transferring control of dual-use encryption to the Department of Commerce specifically states that no right of judicial review is created with this transfer.[82]

[78] Some encryption can only be used for non-communicative purposes. A common example of this is the encryption that is used to encode personal identification numbers (PINs) used at ATMs.

[79] Interim Rule, *supra* note 22, at 67573.

[80] See *infra* Part III.C.

[81] 22 U.S.C. § 2778(h). See *infra* Part III.A., for a discussion of the APA.

[82] "[This order] is not intended to, and does not, create any rights to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural . . .". Clinton Order, *supra* note 50, at § 3.

4. *Regulations Applicable to Software and/or Source Code*

Both the ITAR and EAR impose regulations on encrypting hardware, software, and source code. Regulations governing the export of encrypting hardware almost certainly do not raise First Amendment issues. However, regulations governing software and computer operating instructions known as source code almost certainly do raise First Amendment issues.[83] The EAR defines encryption source code as "[a] precise set of operating instructions to a computer that, when complied, allows for the execution of an encryption function. . . . "[84]

ITAR also regulates software and computer source code. Two recent lawsuits filed against the State Department appealed administrative decisions denying permission to export encrypting source code in print and on diskette.[85] In both suits, the Department of State denied petitioners permission to export encrypting source code.[86] After unsuccessfully appealing the CJR decisions within the State Department, plaintiffs Karn and Bernstein filed suits alleging violations of their constitutionally protected rights. As the standard bearers for the case against regulation of encryption, the *Karn* and *Bernstein* cases illustrate the problems, difficulties and incongruities found in the ITAR regulatory scheme. Due to the underlying similarities between ITAR and EAR, the issues raised in these cases carry through to EAR as well as to all similar future regulatory schemes.

D. Karn v. Department of State[87]

In 1994, Philip J. Karn submitted CJR's to the State Department for a determination of whether two items were subject to the export restrictions of the ITAR.[88] These items were: *Applied Cryptography*,[89] a book on computer encryption widely available throughout the United States; and a computer diskette containing the cryptographic source codes printed in Section V of *Applied Cryptography*, together with programmer's comments interspersed within the code itself. In response to Karn's CJR, the State Department granted permission for the export

[83] *See infra* Part III.B.1.

[84] Interim Rule, *supra* note 22, at 68,585.

[85] Karn v. United States Dep't of State, 925 F. Supp. 1 (D.D.C. 1996); Bernstein v. Department of State, 922 F. Supp. 1426 (N.D. Cal. 1996).

[86] Source code is "merely a means of commanding a computer to perform a function". *Karn*, 925 F. Supp. at 27, n.19.

[87] *Id.* at 1.

[88] *Id.* at 3.

[89] *See* SCHNEIER, *supra* note 12.

of the book, but not the diskette.[90] Karn appealed the decision through the State Department's internal review process and lost.[91] Karn subsequently filed suit in federal district court for the District of Columbia.

In his suit, Karn alleged that the State Department had violated his First and Fifth Amendment rights when it denied him permission to export the diskette.[92] Karn further alleged that the decision to prohibit the export of the diskette was arbitrary and capricious and an abuse of discretion in violation of federal law.[93]

In response to Karn's allegations, the Department of State filed a motion for summary judgment asserting that, under Subsection (h) of the AECA, the court could not hear Karn's claims, and that the licensing scheme had not violated Karn's constitutional rights.[94] The District Court agreed that Karn's APA-based claims were nonjusticiable,[95] and held that the licensing scheme did not violate the Constitution.[96] While Karn's appeal was pending, President Clinton moved control over encryption exports to the Department of Commerce. In light of this move, the D.C. Circuit remanded the case back down to the District Court for a rehearing once the new Export Administration regulations had become effective.[97] After this ruling, Karn needed to resubmit his export petition under the new regulations, this time to the Department of Commerce.

[90] The CJR and Deparpptment of State response is available on-line at (last modified Feb. 5, 1998) <http://www.people.qualcomm.com/karn/export/executive.html>.

[91] *Karn*, 925 F. Supp at 4. For the text of Karn's initial appeal, see (visited Feb. 8, 1998) <http://www.people.qualcomm.com/karn/export/harris_appeal.html>.

[92] *Karn*, 925 F. Supp. at 2.

[93] Karn alleged that the decision was in violation of the Administrative Procedure Act (APA). *Id.* The APA and its relationship to cryptographic export controls is discussed further *infra*, Part III.

[94] *Karn*, 925 F. Supp. at 26.

[95] *Id.* at 8.

[96] *Id.* at 26.

[97] Karn v. United States Dep't of State, 107 F.3d 923 (D.C. Cir. 1997) (unreported opinion).

E. Bernstein v. Department of State[98]

Daniel Bernstein was a Ph.D. candidate in mathematics at the University of California at Berkeley when he developed the "snuffle encryption system." Bernstein wrote source code for the snuffle system and an academic paper describing the system. He sought to publish his academic papers and the text of the source code internationally.[99] In addition, Bernstein sought permission to discuss the paper's contents with foreign nationals who might attend international conferences for mathematicians.[100] Bernstein filed a CJR seeking approval for these activities from the Department of State.

The Department of State refused Bernstein's request for permission to publish and export the text of the source code,[101] prompting him to file suit. Bernstein's complaint sought declaratory and injunctive relief, alleging that the AECA/ITAR licensing scheme amounted to an unconstitutional prior restraint on speech, and was unconstitutionally vague and over-broad.[102] Bernstein, like Karn, also alleged that the decision to deny his petition was arbitrary and capricious and an abuse of power under the APA.[103] The State Department countered with the same argument used against Karn that the APA-based claims were nonjusticiable under the AECA and that denial of Bernstein's CJR amounted to a constitutionally permissible restraint on conduct rather than an unconstitutional restraint on speech.[104]

In the first of three opinions, a California district court judge ruled that Bernstein's computer source code was "speech" for purposes of the First Amendment protection and analysis.[105] In the second of the *Bernstein* opinions, the court held that the imposition of the ITAR export licensing

[98] Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996) (Bernstein I); Bernstein v. United States Dep't of State, 945 F. Supp. 1279 (N.D. Cal. 1996) (*Bernstein II*); Bernstein v. United States Dep't of State, C-95-582, Aug. 25, 1997, 1997 U.S. Dist. LEXIS 13146 (*Bernstein III*).

[99] *Bernstein*, 922 F. Supp at 1430.

[100] *Id.*

[101] Initially, the source code was not on computer diskette, as was the case in *Karn. Bernstein,* 922 F. Supp. at 1429. Originally, the Department of State denied permission to export either the source code or the academic papers. However, once Bernstein had filed suit, the Department of State granted permission to export the academic papers, but not the source code. *Id.* at 1433. After control over encryption moved to the EAR, Bernstein sought permission to export snuffle's source code on diskette as well. EAR liberalized source code export rules when the code is to be distributed in print. *See supra* note 154.

[102] *Id.* at 1430-31.

[103] *Id.*

[104] *Id.* at 1431.

[105] *Id.* at 1436.

requirements on source code "speech" amounted to a violation of the First Amendment.[106] In the third opinion, the court considered whether the newly promulgated EAR encryption regulations were constitutional as applied to Bernstein's source code.[107] Once again, the court struck down the provisions. An appeal has been filed, however, staying the majority of the injunction pending a final ruling by the Ninth Circuit.[108] A new issue is raised on appeal—whether Bernstein may export a computer disk containing the snuffle source code.

In denying the State Department's initial motion for summary judgment, the *Bernstein* court held that source code is speech and that the constitutionally-based claims advanced were justiciable.[109] The *Karn* court decided to treat the contents of the Karn diskette as speech because it included English-language comments, but specifically declined to rule on whether source code alone would be speech. It then ruled that the licensing scheme was constitutionally permissible as a content-neutral restraint on speech.[110] In contrast to the rulings on *Bernstein's* nearly identical claims, the court in *Karn* found that the constitutional claims were, as a matter of law, unsupported.[111]

What follows is a discussion of the constitutional issues raised in *Karn* and *Bernstein*.[112] These issues are: (1) whether the judiciary has the

[106] *Bernstein*, 945 F. Supp. at 1289-90 (discussing the requirements for a constitutional licensing scheme, the court concluded that "[t]he ITAR scheme . . . fails on every count").

[107] Bernstein v. United States Dep't of State, No. C-95-0582, 1997 WL 530866 at *1 (N.D. Cal. Aug. 25, 1997).

[108] Bill Kisliuk, *Patel Again Pokes Hole in Encryption Export Ban*, RECORDER, Aug. 26, 1997, at 1; Wendy R. Leibowitz, *Encryption Regulations Struck By District Court*, NAT'L L.J., Sept. 8, 1997, at A12.

[109] Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1439 (N.D. Cal. 1996).

[110] Karn v. United States Dep't of State, 925 F. Supp. 1, 25-26, 34-35 (D.D.C. 1996). *See also* note 148.

[111] *Id.* at 8-14.

[112] In a third case challenging the ITAR/EAR schemes on constitutional grounds, a law professor at Case Western Reserve University School of Law has brought suit to challenge a determination that posting his course materials on the Internet would violate ITAR/EAR. Professor Peter Junger sought to make encryption materials available to his students over the Internet for a class titled "Computers and the Law." The Internet materials, made available through a Web site, included an encrypting application. After he asked the State Department whether his materials fell within the ITAR, the Department decided that the posting of encrypting applications on the Internet was tantamount to "publication," and therefore within the scope of the ITAR.

authority to hear challenges to encryption licensing decisions, (2) whether the encryption restraints impinge on conduct or speech, (3) whether the encryption licensing restraints are content-based or content-neutral, and (4) if the encryption licensing scheme is a restraint on speech, whether national security concerns remove the source code from the realm of "protected speech."

III. CONSTITUTIONAL ISSUES

A. *Justiciability of Encryption Regulations and National Security*

In both *Karn* and *Bernstein*, the plaintiffs asserted that the judiciary had federal question jurisdiction under the Administrative Procedure Act of 1946 (APA)[113] and under the United States Constitution.[114] In its reply, the State Department argued that the decision to include or exclude certain items from the USML was a nonjusticiable issue under the 1989 amendment to the AECA that purports to bar judicial review of USML classification decisions.[115] The threshold issue that challenges to the regulatory scheme raise then is whether the judiciary has the power to review the actions of the State Department in the instant case. This power to review, if present, comes from either the APA, the Constitution, or both.

Except where the Constitution requires it or where legislation permits it, there are no constitutionally guaranteed rights to judicial review of legislation, administrative rules, or regulatory decisions.[116] In 1946, Congress created a presumptive right to judicial review of administrative decisions with the APA.[117] Section 701 of the APA creates the right of judicial review of all governmental agencies and their decisions,

Since this initial CJR determination, Mr. Junger has appealed, filed suit, and, most recently, amended his complaint to include the Department of Commerce under the EAR. The complaint and its legal arguments closely mirror the *Karn* and *Bernstein* complaints. Mr. Junger alleges that the regulations amount to an unconstitutional prior restraint on free speech, and that encryption source code and software is more akin to protected speech than functional conduct (last modified Sept. 3, 1997) <http://samsara.law.cwru.edu/comp_law/crypto_export/>.

[113] Codified at 5 U.S.C. §§ 701-706 (1989 & Supp. 1995).

[114] Karn v. United States Dep't of State, 925 F. Supp. 1, 3; Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1431 (N.D. Cal. 1996).

[115] Karn, *Points & Authorities*, *supra* note 8, at 11-16.

[116] Estep v. United States, 327 U.S. 114 (1946).

[117] 5 U.S.C. §§ 701-706 (1989 & Supp. 1995).

except in cases where Congress has expressly precluded judicial review in the text of a statute.[118]

In 1989, Congress amended the AECA by adding Subsection (h).[119] This subsection explicitly bars judicial review of classification decisions under the ITAR and the AECA.[120] In the case of APA-based claims against the AECA, the 1989 addition of Subsection (h) removes the Act from the scope of the APA.

In 1990, The Eleventh Circuit Court of Appeals relied on Subsection (h) when it refused to hear a challenge to a CJR determination in *United States v. Martinez.*[121] The *Martinez* court held that challenges to encryption export license decisions were beyond the province of the court, commenting that "[t]he question whether a particular item should have been placed on the Munitions List possesses nearly every trait that the Supreme Court has enumerated [that] traditionally renders a question 'political'."[122] However, the court in *Martinez* noted that the parties had not raised any constitutional challenges to the CJR.[123] The court held that encryption export licensing decisions are the domain of the Executive Branch, but left open the possibility of constitutionally based challenges, notwithstanding the limitations on judicial review imposed under Subsection (h).[124] Presumably, this ruling would apply as well to any successor to the AECA that purported to bar judicial review.

[118] Webster v. Doe, 486 U.S. 592, 599 (1988) ("[s]ection 701(a), however, limits application of the entire APA to situations in which judicial review is not precluded *by statute.*") (emphasis added).

[119] Pub. L. 101-222 § 6.

[120] Subsection (h), entitled "Judicial Review of Designation of Items as Defense Articles or Services," states:

> The designation by the President (or by an official to whom the President's functions under subsection (a) have been duly delegated), in regulations issued under this section, of items as defense articles or defense services for purposes of this section shall not be subject to judicial review.

22 U.S.C. § 2778(h) (1994).

[121] United States v. Martinez, 904 F.2d 601, 602 (11th Cir. 1990).

[122] *Id.*

[123] *Id.* at 603.

[124] *Id.*; *see also* INS v. Chada, 462 U.S. 919, 941-42 ("No policy underlying the political question doctrine suggests that Congress or the Executive, or both acting in concert and in compliance with Art. I, can decide the constitutionality of a statute; that is a decision for the courts."); Smith v. Maryland, 442 U.S. 735, 740, n.5 (1979); National League of Cities v. Usery, 426 U.S. 833, 841, n.12 (1976); Buckley v. Valeo, 424 U.S. 1 (1976); Myers v. United States, 272 U.S. 52 (1926); Marbury v. Madison, 1 Cranch (5 U.S.) 137, 180 (1803) ("A law repugnant to the constitution is void.").

Thus Karn's and Bernstein's APA-based claims appealing ITAR decisions appear to be blocked by Subsection (h). However, their constitutionally-based claims may be heard if the court finds the CJR determinations to be outside of the political question doctrine.

The new encryption regulations governed by the EAR do not seem to preclude judicial review of administrative licensing decisions. However, President Clinton's executive order transferring control from the State Department to the Commerce Department specifically states that no rights of judicial review or administrative review are created with the transfer.[125] The Court's opinion in *Webster v. Doe* seems to state that only Congress can preclude APA-based review.[126] Since the underlying legislation empowering the Executive Branch to control these commodities does not create APA preemption,[127] it appears that the invocation of the preemption is an act of executive fiat. Thus, the language of the Clinton order should not be read as a limit on judicial review, but rather as a disavowal of any intention to expand on any rights to review.

Nevertheless, the existence of a right of review does not necessarily oblige a court to hear the case. A court may decline to hear a challenge to an administrative action if the issue falls within the political question doctrine, and the court finds itself ill-equipped to render a judgement on the merits. The most frequently cited definition of the scope of the political question doctrine was stated by the Supreme Court in *Baker v. Carr*.[128] Justice Brennan, writing for the Court in *Baker*, announced two key factors that courts should consider in deciding whether they have the proper authority to review the actions of another branch of the federal government.[129] These factors are: (1) whether there is a "textually demonstrable constitutional commitment of the issue to a coordinate political department," and (2) whether there is a "lack of judicially discoverable and manageable standards for resolving" the issue.[130]

[125] *See supra* note 82 and accompanying text.

[126] *See supra* note 118.

[127] Although APA preemption exists under the AECA/ITAR scheme, no such right of preemption exists under the EAA/EAR scheme. 22 U.S.C.A. § 2778(h) (West 1991).

[128] Baker v. Carr, 369 U.S. 186 (1962), *on remand* 206 F. Supp. 341 (M.D. Tenn. 1962).

[129] *Id.* at 217. Note that these factors are disjunctive. Satisifaction of one or the other could be enough to trigger the political question doctrine and render an issue nonjusticiable.

[130] *Baker*, 369 U.S. at 217.

1. Commitment to Coordinate Political Branch

It is well established that issues of national security and foreign relations like those raised in *Karn, Bernstein,* and *Junger*[131] are traditionally given over to the Executive Branch.[132] Nevertheless, although the Executive Branch has dominion over these issues[133] and its decisions in these areas are generally beyond judicial review, "judgment concerning the 'political' nature of even a controversy affecting the Nation's foreign affairs is not a simple mechanical matter."[134] One can see this flexibility in the fact that the judiciary has, on a number of occasions in the past, heard challenges to Executive decisions that dealt with national security or foreign affairs concerns.[135] Thus, precedent suggests that Brennan's statement that a constitutional grant of power to a coordinate political branch of government invokes the political question doctrine has not been applied strictly in the years since it was first written. In fact, Brennan rejected the argument that

[131] *See supra* note 112.

[132] This principle was underscored by the Supreme Court in 1936:

> As Marshall said in his great argument of March 7, 1800, in the House of Representatives, "The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." Annals, 6th Cong., col. 613. The Senate Committee on Foreign Relations at a very early day in our history (February 15, 1816), reported to the Senate, among other things, as follows: "The President is the constitutional representative of the United States with regard to foreign nations. He manages our concerns with foreign nations . . . ".

United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936).

In some cases, Congress has added to the Executive branch's authority and autonomy with the passage of legislation that purports to grant wide discretion in matters related to national security. In the *Webster* case, Congress expressly granted great discretion to the Executive branch in dealing with the hiring and firing of CIA employees, allowing the director to terminate an agent's employment, "whenever he [the Director] shall deem such termination necessary or advisable in the interests of the United States." Webster v. Doe, 486 U.S. 592, 594 (1988) (citing National Security Act of 1947 § 102(c) (codified at 50 U.S.C. § 403(c))).

[133] U.S. CONST., art. II, § 2.

[134] Baker v. Carr, 369 U.S. 186, 283 (1962).

[135] *See e.g.,*Webster v. Doe, 602 F. Supp. 581, 582 (1986); *rev'd,* 796 F.2d 1508 (D.D.C. 1986); *aff'd in part and rev'd in part, remanded,* 486 U.S. 592 (1988), *on remand,* 859 F.2d 241 (D.D.C. 1988); New York Times Co. v. United States, 403 U.S. 713 (1971); United States v. Progressive, Inc. 467 F. Supp. 990 (W.D. Wis. 1979).

anything simply touching national security was beyond the judiciary's power of review.[136]

2. *Judicially Discoverable and Manageable Standards*

Likewise, a lack of judicially discoverable and manageable standards by which to judge the constitutionality of the actions of the Executive has been, in practice, a less than dispositive factor in deciding whether to invoke the political question doctrine. In *Webster v. Doe*, the Court remanded to a district court for a determination whether the CIA director's decision to fire an employee for his potential risk to security violated the employees' constitutional rights.[137] In the *Progressive* case, a federal district court reviewed sensitive information about the construction of a hydrogen bomb and found publication of the information to pose a threat to national security.[138] Finally, in *New York Times, Co. v. United States*, a divided Court reviewed sensitive Pentagon documents regarding the United States involvement in Vietnam and Cambodia during the Vietnam War. The Court decided per curiam that because the government had not sufficiently demonstrated the necessity of the prayed-for injunction, the Court would not permit its issuance.[139] In all of these cases, the plaintiffs asked the courts make difficult determinations about a potential threat to national security despite the fact that the courts lacked the expertise to make these determinations. Nevertheless, the courts reviewed these cases on their merits, rather than invoke the political question doctrine and defer to the judgment of the better-informed branch: the Executive. It is clear then that courts have not blindly applied Brennan's test announced in *Baker*. However, this conclusion begs the question of when courts will apply the test and when they will not.

Although the Supreme Court has never directly addressed this issue, it appears that the nature of the plaintiff's claim dictates the standard of review to be applied when determining justiciability. Thus, the familiar standards of review such as rational relation[140] and strict scrutiny,[141] which require an examination of the relationship between the

[136] *Baker*, 369 U.S. at 211.

[137] *Webster*, 486 U.S. at 605.

[138] *Progressive, Inc.*, 467 F. Supp. 990.

[139] *New York Times*, 403 U.S. at 714.

[140] Kadrmas v. Dickinson Pub. Sch., 487 U.S. 450, 462 (1988) ("a statute is upheld if it bears a rational relation to a legitimate government objective.").

[141] The rights of a free press and free speech are "fundamental" for purposes of constitutional law analysis. State actions violating fundamental rights require strict scrutiny. Thornburgh v. American College of Obstetricians & Gynecologists, 476 U.S. 747, 782, 774 n.3 (1986).

government's action and the plaintiff's complaint, are implicitly applied to justiciability determinations while expressly applied to the issue of constitutionality. In terms of practical effect, these two applications merge into a single application, with a finding of unconstitutionality necessarily predicated on a finding of justiciability. This consistency between justiciability standard of review and constitutionality standard of review is necessary when one considers the alternative: an application of a single standard of review applied to all cases. Such single standards would either take the form of a presumption of justiciability (akin to a strict scrutiny standard), or a presumption of nonjusticiability (akin to a rational relation standard).

If the courts presumed nonjusticiability for cases touching national security,[142] it appears the courts would never have heard the cases discussed above: *New York Times*, *Progressive*, and *Webster*. In all of these cases, the governmental action appears to bear a rational relation to the interest of protecting national security.[143] Applying a rational relation standard to determine justiciability would virtually bar the courts from hearing any cases which touched on national security issues. On the other hand, universal application of a presumption of justiciability would serve to expand the number of cases reviewable by the courts and would likely permit review of many cases that are properly entitled to the benefit of the political question doctrine.

It therefore appears that the criteria to be used when deciding justiciability extend beyond the mere presence or absence of "judicially discoverable and manageable standards" and any constitutional commitments to "coordinate political branches." Courts making justiciability determinations also consider (with or without a conscious acknowledgment) the nature of the claim brought by the aggrieved party. In the cases of *Karn* and *Bernstein*, if the regulations are content-based, and if source code is speech, then the court should apply a strict scrutiny

[142] This standard might be applied in an effort to defer to the judgement of the Executive branch in these matters.

[143] In *New York Times*, the publication of sensitive documents about the United States' involvement in the Vietnam war could have had an impact on national security or foreign relations. In the *Progressive* case, publication of previously secret details on how to make a hydrogen bomb posed a very real threat to national security. In *Webster*, the firing of a CIA employee following a determination that his homosexuality posed a threat to security might have been rationally related to national security when the CIA had determined that personal secrets like that of homosexuality can be exploited by enemy agents.

standard of review to the issues of justiciability and constitutionality.[144] In practice however, these tests will merge into one.

B. Is the Restraint Constitutional?

The government has advanced several arguments rebutting the constitutional challenges made by Karn and Bernstein. The State Department has argued that the licensing scheme restrains non-expressive conduct rather than speech, making a First Amendment regulation of speech analysis inappropriate.[145] The State Department has also argued that it regulates the source code because of its functional capabilities rather than because of any ideas or beliefs expressed in the code,[146] essentially arguing that the restraint is content-neutral.[147] The first argument, centering around the issue of whether source code is speech, is discussed in the following Part.

1. The Nature of Source Code: Is it "Speech" or "Conduct?"

The court in *Karn* expressly avoided ruling on the issue of whether computer source code by itself is speech for purposes of constitutional analysis.[148] The Supreme Court has recognized that the First Amendment protections of speech and of the press are not subject to a literal reading and were meant to include other modes of expression.[149] Recognizing that all acts of speaking are imbued with some element of

[144] *See infra* Part III.B.2.

[145] Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1434 (N.D. Cal. 1996).

[146] Karn, *Points & Authorities*, *supra* note 8, at 23.

[147] *Bernstein*, 922 F. Supp. at 1436-37 (defendants urging the adoption of the *O'Brien* content-neutral standard); Karn v. United States Dep't of State, 925 F. Supp. 1, 10 (D.D.C. 1996) (court accepted defendant's contention that regulations are content-neutral).

[148] *Karn*, 925 F. Supp. at 27 n.19. For purposes of its discussion the *Karn* court assumed that source code together with programmer's comments would qualify as speech. The computer disks at issue in *Karn* contained source code for cryptographic algorithms found in the companion book APPLIED CRYPTOGRAPHY. The disks also contained, interspersed with the source code, explanatory comments in a form readable by humans, information that would be ignored by a computer running the code, but helpful to a person studying the code. *Id.* at 26. Because the disks contained both source code and "comments" the court was willing to assume that the contents of the disk were speech for purposes of constitutional analysis, without ruling on the constitutional status of the source code itself.

[149] Superior Films, Inc. v. Department of Educ., 346 U.S. 587, 589 (1954) (addressing the applicability of the First Amendment to motion pictures, the Court wrote, "Motion pictures are of course a different medium of expression than the public speech, the radio, the stage, the novel, or the magazine. *But the First Amendment draws no distinction between the various methods of communicating ideas.*") (emphasis added).

conduct, the Court has extended First Amendment protection to expressive conduct, but declined to extend the full protection of the First Amendment to non-expressive conduct.[150]

In both *Bernstein* and *Karn*, the State Department asserted that cryptographic source code was not "speech," but rather non-expressive conduct that is not afforded any protection under the First Amendment.[151] From these cases, it is reasonable to conclude that the determination whether an encryption export regulation impinges on speech or conduct requires consideration of the following factors: (a) the medium of recordation; (b) the act of exporting and the "conduct" of delivering a message; (c) the nature of source code; and (d) the rationale for regulating encryption.

a. Medium of Recordation

In answering Karn's CJRs, the State Department granted permission to export a book that contained the very same encrypting algorithms found on the companion computer disk.[152] The only difference between the contents of the disk and the corresponding contents of the printed materials was the medium on which they were recorded.[153] It appears that the State Department decided to treat the disk differently because of the difference in medium of recordation. In a similar fashion, the Department of Commerce has adopted a rule that treats encryption recorded in print differently from encryption recorded in any other medium.[154] Analytically, one must begin by deciding whether bits of data, encoded on a magnetic medium such as a computer disk qualify as

[150] Texas v. Johnson, 491 U.S. 397, 402 (1989) (Justice Brennan noting that, as a threshold issue, the Court must "first determine whether [defendant] Johnson's flag burning constituted *expressive* conduct, permitting him to invoke the First Amendment in challenging his conviction") (emphasis added).

[151] Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1434 (N.D. Cal. 1996); Karn, *Points & Authorities*, *supra* note 8, at 13.

[152] *Karn*, 925 F. Supp. at 3.

[153] Letter dated December 5, 1994 from Kenneth C. Bass, III and Thomas J. Cooper (Karn's attorneys) to Thomas E. McNamara, Assistant Secretary, Department of State, Bureau of Politico-Military Affairs (visited Feb. 8, 1998) <http://www.people.qualcomm/karn/export/mcnamara_appeal.html/>.

[154] Encrypting software that would otherwise be subject to the EAR licensing scheme is exempt from the export review requirements if it is distributed in print as a book. *See* 15 C.F.R. § 734.3, Notes to Paragraphs (b)(2) and (b)(3) (1997).

"speech." If they do not, they are not eligible for the protection of the First Amendment.[155]

It would seem that printed words do not lose their character as speech once they are recorded in a machine-readable medium such as a computer disk. Were Mr. Bernstein or Mr. Karn to stand on a street corner and hand out copies of the Communist Manifesto to passersby, their actions would constitute "speech" for purposes of constitutional analysis. If they were to print the Manifesto in a foreign language like French or German, the degree of protection to which they would be entitled should not change.[156] Likewise, the protected status of the publication should not change if the Manifesto were contained on an audio cassette, microfiche, or on a computer diskette.

In the case of the Manifesto being printed in a foreign language, the mere fact that its words are unintelligible to many would-be readers does not take away from the fact that it is still speech. Likewise, reading the Manifesto onto an audio cassette, printing it on microfiche, or typing it onto a diskette should not remove the document from the realm of "speech" merely because the document is unintelligible to the unaided ear or eye. Courts should accord all recorded information the same degree of protection whether memorialized on paper, microform, audio cassette or computer disk. The fact that the source code in *Karn* is recorded on a computer diskette does not make the information something other than speech. Similarly, the encrypting source code on Professor Junger's Web page should be treated as speech, even though the data exists as a string of 1s and 0s in the ephemeral realm of cyberspace.[157] In addition to finding support in constitutional law decisions, another area of law supports the conclusion that information imprinted on a computer diskette is "speech."[158]

United States copyright law regards computer source code as a "literary work."[159] Congress defined literary works as "works, other

[155] This initial inquiry focuses on whether information recorded on a computer disk can ever be considered "speech" for First Amendment purposes. The content of the information, which might be anything from Shakespeare to a spreadsheet program, is irrelevant to this inquiry. The issue of content is addressed *infra* in Part III.B.1.c.

[156] The right to speak foreign languages is likely protected under the 14th Amendment's implicit guarantee of the right of "privacy." See Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (protecting the right to teach a foreign language). The Ninth Circuit has taken this even further, striking down a provision of the Arizona Constitution which made English the official State language. Yniquez v. Arizonans for Official English, 69 F.3d 920, 934-35 (9th Cir. 1995), *vacated and remanded on other grounds*, 117 S. Ct. 1055 (1997).

[157] For a description of Mr. Junger's case, see *supra* note 110.

[158] 17 U.S.C. §§ 101-1101 (1994).

[159] 17 U.S.C. § 101 (1994).

than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phono records, film, tapes, disks, or cards, in which they are embodied."[160] When it passed the Copyright Act in 1976, Congress had the foresight to extend copyright protection to any medium of recordation then known, and to any recording medium later developed.[161] Thus, it is clear that the Act extends copyright protection based on the content of the literary work, and not based on the author's chosen medium of recordation.

In *Bernstein*, the court analogized speech protected by the First Amendment to literary works protected under copyright law. The court noted that copyright law does not protect an idea itself, but rather the expression of that idea; just as the First Amendment protects the expression of ideas. The expression protected "connotes the 'speaking' of an idea."[162] The court went on to note that, "[w]hile copyright and First Amendment law are by no means coextensive, and the analogy between the two should not be stretched too far, copyright law does lend support to the conclusion that source code is a means of original expression," and as such should be regarded as "speech" for purposes of constitutional analysis.[163] It would seem then, that data recorded in an electronic medium like a computer disk would ordinarily be entitled to the full protection of the First Amendment. In certain instances, however, certain media have unique traits such that increased governmental regulation is permitted where identical regulations would not stand in other media.[164] Whether computer disks or other machine-readable media have such traits is the second issue that must be addressed when analyzing the effect of the medium of recordation.

[160] *Id.*

[161] *Id.*

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

[163] *Id.*

[164] Red Lion Broad. Co. v. Fed. Communications Comm'n, 395 U.S. 367, 390-92 (1969) (holding that the FCC may require broadcasters to provide equal time for opposing political views because the useable range of broadcast frequencies is limited); *but see* Times Film Corp. v. Chicago, 365 U.S. 43, 51 (1961) ("I am aware of no constitutional principle which permits us to hold that the communication of ideas through one medium may be censored while other media are immune.") (Warren, C.J., dissenting); *see also supra* note 143.

In *Karn*, the government had argued that computer disks carrying source code are functionally different from books containing source code.[165] The source code on Karn's diskette could be read by a computer, run through a compiler, and turned into object code in a few short steps.[166] Turning the source code in the book *Applied Cryptography* into operating object code required the additional step of entering the source code into a computer, either by typing or scanning the text of the book. The government argued that because Karn's disks facilitated the process of creating working encryption, the disks could be regulated in a way that might not be allowed for print media.[167]

It is undeniable that the information contained on the disks could be converted to a working program more easily than the information contained in print. However, there ought not to be anything magical about data on disks. In *Red Lion*, the Court focused on the scarcity of the broadcast frequencies.[168] This scarcity required that the airwaves be regulated in a way that print media need not be. At the time, it was thought that no other medium could fairly substitute for radio and television broadcasting.[169] There are no traits that inhere in computer disks that are analogous to broadcasting in terms of scarcity or uniqueness. Information in print can easily be converted to computer-readable data and electronic media can easily be converted to print. The greater the ease of this conversion, the more the two media ought to be treated in a similar fashion. Ultimately, the impact of the medium of recordation should be measured when considering the applicability of the national security override, discussed *infra* in Part III.D. When one medium is only a whisper away from transformation into the second medium, the national security analysis for one should suffice for both. However, where a great deal of time, effort, skill or expense is required to transform information embodied in one medium to another medium, the national security analysis taken up in Part III.D. *infra* should be bifurcated.[170]

[165] Karn v. United States Dep't of State, 925 F. Supp. 1, 14 (D.D.C. 1996).

[166] Presumably, Karn intended that purchasers of his source code companion disks would run through this process to obtain working encryption. For an explanation of the relationship between source code and operational software, see *supra* note 52.

[167] Declaration of William P. Crowell, Deputy Director of National Security Agency (visited Feb. 8, 1998) <http://people.qualcomm.com/karn/export/crowell.html> (detailing the functional differences between in-print source code and the source code on the Karn disk).

[168] *Red Lion Broad. Co.*, 395 U.S. at 389-92.

[169] Technology, with the proliferation of cable television and the Internet, has since proven the Court's concerns to be unfounded.

[170] A simple example illustrates this point. Imagine someone offering for sale (1) copies of a high quality photograph of a $100 bill, and (2) sets of printing plates

In this case, the information contained in print can be transformed into a machine-readable format through typing, scanning, or even through computer voice dictation. The source code algorithms in *Applied Cryptography*, though numerous, are not lengthy and could likely be reproduced in their entirety in a few hours. No significant degree of skill is required for this transformation. As a result of the close proximity of print media and machine-readable media, the two should be treated the same. If one medium is protected by the First Amendment, so too should the other be protected. The medium of recordation by itself cannot stand as grounds on which the government's actions may find support in this case.

b. *The Act of Exporting*

At issue in both *Bernstein* and *Karn* is the right to export information.[171] The Department of State, in its Memorandum of Points and

engraved with the same image. In response to this person's marketing efforts, the government seeks an injunction on the grounds that the images for sale can be used to counterfeit US currency. The salesman offers the First Amendment as the basis for his defense. Both the photograph and the engraved plates render the same images. However, while it is clear that an injunction barring the sale of the plates may well be granted, it is not clear that the sale of the photographs will enjoined as well. One possible reason for this disparate treatment is the degree of skill and effort that is required to produce the plates. The photographs are not easily converted to printing plates. Imagine now that the same person is selling computer disks containing a scanned version of the photograph. The photograph can easily be converted to a machine-readable format with a common scanner, available in homes, offices, copy shops, and schools. Although the scanned image could be used to counterfeit currency on a computer while the photograph by itself is of little use to a counterfeiter, the propriety of the injunction for the photograph and the disks should be decided together. If the scanned image can be easily used to create counterfeit currency, then the sale of the disks as well as the photograph should be enjoined. Likewise, if the photograph is protected by the First Amendment, so too should be the disks since one is so easily transformed into the other.

[171] In *Junger*, the apparent intent of the petitioner was merely to make his class materials available over the Internet, an act which was considered an "export" under the EAR since foreign parties could access this information. *See supra* note 112 and accompanying text. For the purposes of this discussion, "export" does not necessarily mean transactions engaged in for profit. The AECA/ITAR regulations do not distinguish between commercial activities and non-commercial activities; they are applied without discrimination to Mr. Bernstein's and Mr. Junger's academic "exports" and Mr. Karn's commercial "exports." For purposes of constitutional analysis, Mr. Karn's sale of the diskettes did not, by placing his activity in the commercial realm, automatically limit applicability of First Amendment protections to his speech. Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 501 ("books, newspapers, and magazines are published and sold

Authorities seeking to have Karn's case dismissed, implies that the act of exporting is conduct unrelated to speaking and is therefore not entitled to First Amendment protection.[172] By arguing that the export controls do not restrict expression, but rather merely restrict an act (exporting), the government draws a distinction between speaking and the act of exporting. Although speaking and exporting are not the same, neither are the two mutually exclusive. The speech/conduct distinction brought up by the State Department does not turn on the act of exportation.

Communicating to an audience abroad is generally within the scope of the First Amendment.[173] However, if international communication threatens national security, the First Amendment does not protect it.[174] Courts have also upheld restraints based on national security that were imposed on media with a primarily domestic circulation, presumably aimed at a primarily domestic audience.[175] It appears then that the audience to which the speech is directed is not as important as the content of the speech, because threats to national security exist both domestically and abroad.[176] The issue of whether encrypting source code endangers national security is taken up in Part III.D., *infra*.

Every act of "speaking" necessarily contains some elements of conduct. Forcing air across one's vocal chords or distributing a newspaper are both forms of conduct, but are also necessary antecedents to the act of "speaking." "Speaking" cannot be completed without the ability to deliver one's message, whether it be vocally or through a more elaborate distribution scheme.

For example, all newspapers employ some sort of delivery process to get the news from the printing presses to the newsstand. Suppose that the government permitted news gathering, writing and publication, but prohibited the distribution of newspapers. Clearly, such a regulation would have the effect of quashing the freedom of the press, even though it was aimed only at the non-communicative conduct of distribution.[177]

for profit [but that] does not prevent them from being a form of expression whose liberty is safeguarded by the First Amendment").

[172] "Control over . . . [encryption source code] export does not restrict expression, but [rather] the conduct of exporting a functioning defense article." Karn, *Points & Authorities, supra* note 8, at 6.

[173] Bullfrog Films, Inc. v. Wick, 847 F.2d 502, 511-12 (9th Cir. 1988) (noting that First Amendment protection is the same when speech is aimed abroad as when it is aimed a domestic audience).

[174] *Id. See also infra* Part III.D.

[175] *See* United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wisc. 1979).

[176] The advent of home-grown terrorism like the bombings in Oklahoma City and Atlanta supports this contention.

[177] *See* Lakewood v. Plain Dealer Pub. Co., 486 U.S. 750, 762-69 (1988); Griswold v. Connecticut, 381 U.S. 479, 482 (1965) ("The right of freedom of speech and

The EAR/ITAR regulations essentially function on this level, permitting scientists, mathematicians and others to research, write and publish scientific and technical data in the United States, while prohibiting distribution beyond our borders through certain channels without first obtaining a censor's stamp of approval.

The First Amendment must carry with it an implied protection on the acts related to and necessary for expression.[178] Recognizing this self-evident principle, and recognizing that exportation of a writing is simply a method of delivering one's message to an audience abroad, it is apparent that an analysis of the constitutionality of the EAR/ITAR restraints should not turn on the act of exportation. The act of exporting should be entitled to the full protection of the First Amendment unless there is something in the content of the message that removes it from this protection.

c. *The Nature of Source Code*

Interpreting the scope of the First Amendment, the Supreme Court has on a number of occasions deemed acts imbued with symbolic meaning to be within the aegis of the First Amendment.[179] These symbolic acts, termed "expressive conduct," are protected by the Bill of Rights while acts devoid of expression are not.[180]

The *Bernstein* court noted that the expressive conduct test applied by the Court in *Texas v. Johnson* seemed to apply only "in the absence of the 'spoken or written word'."[181] Relying on language from *Texas v. Johnson* and *Spence v. Washington*,[182] the district court in *Bernstein*

press includes not only the right to utter or to print, but the right to distribute, the right to receive, [and] the right to read . . . . Without those peripheral rights, the specific rights would be less secure.")

[178] *Griswold*, 381 U.S. at 482.

[179] *See, e.g.*, Tinker v. De Moines, 393 U.S. 503, 505 (1969) (protection for the wearing of a black armband to protest the Vietnam war); Spence v. Washington, 418 U.S. 405, 409-11 (1974) (protection for the display of an American Flag with a peace symbol taped on it); Texas v. Johnson, 491 U.S. 397, 404 (1989) (protection for the burning of a flag outside of the Republican National Convention); *but cf.* California v. LaRue, 409 U.S. 109, 118 (1972) (conduct of nude barroom dancing afforded only minimal First Amendment protection).

[180] *Texas*, 491 U.S. at 404.

[181] Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1434 (N.D. Cal. 1996) (citing Texas v. Johnson, 491 U.S. at 404).

[182] *See Spence*, 418 U.S. at 409.

opined that analysis of the communicative content of an act follows only after determining that the act was conduct and not speech:

> In the instant case, Bernstein's encryption system is written, albeit in computer language rather than in English. Furthermore, there is little about this functional writing to suggest it is more like conduct than speech. A computer program is so unlike flag burning and nude dancing that [the government's] reliance on conduct cases is misplaced. It would be convoluted indeed to characterize the snuffle system as conduct in order to determine how expressive it is when, at least formally, it appears to be speech.[183]

Thus it appears that a court reviewing encryption export license determinations for source code need not involve itself in the question of whether the source code is expressive, so long as it is written. In *Karn*, the plaintiff recorded the source code on a computer diskette. Although Karn's source code was not recorded on paper,[184] it is a tenuous proposition to assert that written speech can be transformed into "conduct" merely by recording it on a different medium.

Attorneys for the State Department argued that the source code is a "functioning cryptographic product, [and] is not intended to convey a particular message" and therefore should be regarded as conduct rather than speech.[185] Attacking the philosophic underpinnings of the government's argument, the district court in *Bernstein* noted that the First Amendment protects functional speech. "Thus even if . . . source code . . . is essentially functional, that does not remove it from the realm of speech. Instructions, do-it-yourself manuals, recipes, even technical information about hydrogen bomb construction . . . are often purely functional; they are also speech."[186]

The source codes at issue in *Karn* and *Bernstein* are essentially functional how-to manuals, enabling readers to talk in secret. As the *Bernstein* court noted, however, functional speech is entitled to the same protections as persuasive or communicative speech.[187]

In support of this contention, the *Bernstein* court cited *United States v. Progressive, Inc.*[188] Not cited, but also on point are the watershed concurring opinions written for the "Pentagon Papers" case in 1971.[189]

[183] *Bernstein*, 922 F. Supp at 1434-35.

[184] Mirroring their view of the *Karn* disk, the regulators of the commodity in *Junger* focussed on the fact that it was recorded in an electronic medium (a "Web page") and was accessible and viewable only with the aid of a computer.

[185] *Id.* at 1434.

[186] *Id.* at 1435.

[187] *Id.* Informative speech is protected as well. New York Times Co. v. United States, 403 U.S. 713, 717 (1971) ("The press was protected so that it could bare the secrets of government and *inform the people.*") (Black, J., concurring) (emphasis added).

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

[189] New York Times Co. v. United States, 403 U.S. 713 (1971).

In both cases, the government sought an injunction to prevent the publication of informative articles.[190] In neither case did the court so much as mention that the First Amendment defense raised by the publishers was inapplicable due to the informative rather than persuasive content of the articles.

The proper inquiry in determining whether the EAR/ITAR regulations impinge on speech or conduct is not an analysis of the medium, message, or act of exporting. Rather, the proper inquiry should focus on the rationale behind continuing to regulate source code.[191] In the past, courts have looked to the purpose of a particular regulation to determine whether the regulation impinges on conduct or expression.[192]

2. *Is the Regulation Content-Based or Content-Neutral?*

When a court faces a constitutional challenge to a regulation, "[t]he rationale for a regulation determines the level of scrutiny to be applied . . . [I]f the regulation is content-based, the regulation will be 'presumptively invalid,' whereas if the regulation is content-neutral, then the government may justify the regulation if certain other criteria are met."[193] Therefore, determining regulation rationale is central to the broader question of whether a restraint is constitutional. An example of a content-neutral restraint can be found in the case *Clark v. Community for Creative Non-Violence.* In *Clark*, a Washington, D.C. ordinance prohibited any camping in either Washington D.C.'s Lafayette Park or the Mall.[194] A homeless rights activist group filed suit for infringement of its First Amendment rights when prevented from camping overnight in the Mall in protest of the plight of the homeless in America.[195] In determining whether the ordinance amounted to an

[190] United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979) (how to build a hydrogen bomb); *New York Times Co.*, 403 U.S. 713 (information about the United States' incursions into Cambodia during the Vietnam War).

[191] Clark v. Community for Creative Non-Violence, 468 U.S. 288, 293 (1984) (to be valid, a regulation impinging on symbolic conduct must, inter alia, be unrelated to restricting speech and must be narrowly tailored to serve a substantial government interest. This standard suggests that intent is a relevant factor).

[192] *Id.*; United States v. O'Brien, 391 U.S. 367, 377 (1968) (noting that a law that has the effect of suppressing speech may be unconstitutional if the government in fact sought to suppress free expression).

[193] R.A.V. v. St. Paul, 505 U.S. 377, 382 (1992).

[194] *Clark*, 468 U.S. at 290.

[195] *Id.* at 291-92.

unconstitutional restraint on expression, the Court analyzed the restraint as a time, manner or place restriction and applied a three-prong test.[196] To pass constitutional muster, the restraint must (1) be imposed without reference to the content of the speech, (2) serve a significant government interest and be narrowly tailored to serve that interest, and (3) leave available alternative means of communication.[197]

In analyzing the first prong, the Court found that the prohibition was content-neutral, because anyone wishing to camp overnight was prohibited, regardless of the would-be camper's reason for wanting to spend the night.[198] The Court found the ordinance, on its face and in its application, to be content-neutral.[199] Surprisingly, the court in *Karn* found the ITAR restraints to be content-neutral. It is puzzling how the court made this determination when the EAR/ITAR restraints are, on their face, content-based regulations and it is the content of the source code (its strength) that created the controversy in the *Karn* case.

In analyzing whether a restraint on speech is content-based, a court will look first to the face of the statute or rule in question. A finding that the regulation is facially content-based will render the regulation presumptively invalid.[200] However, even if the regulation is found to be content-neutral on its face, a court will inquire into the intent of the drafters of the rule to determine if it was promulgated in a neutral tone but with suppression of certain content in mind.

a. *Facial Review*

If Bernstein or Karn had written source code for a tic-tac-toe game, presumably the State Department would not have imposed any restraints on the exportation of their wares. Likewise, if Karn or Bernstein had tried to export weak encrypting source code with a key length of less than 40 bits (symmetric), the Departments of State and Commerce would have granted them permission to export.[201] However, because the

[196] *Id.*

[197] *Id.* at 293.

[198] *Clark*, 468 U.S. 288, 295 n.6 (1984).

[199] *Id.*

[200] R.A.V. v. City of St. Paul, 505 U.S. 377, 381-403 (1992); City of Laude v. Gilleo, 114 S. Ct. 2038, 2047 (1994) ("With rare exceptions, content discrimination in regulations of . . . speech . . . is presumptively impermissible, and this presumption is a strong one.") (O'Connor, J., concurring).

[201] The State Department routinely permited "fast track" export of encrypting programs with key lengths under 40 bits symmetric and 512 bits asymmetric. Fahn, *Export FAQ*, *supra* note 22, at 6. The Commerce Department adopted a similar rule, permitting, without a license, export of keys under 40 or 512 bits. Interim Rule, *supra* note 22.

source code enabled readers to securely encrypt their communications, the State Department ruled that the items were subject to export restraints.[202] In essence, the government is permitting a mathematician to utter "x^2" but not "x^3." Just as in *Clark* where the regulation prohibited all camping, the government would have to seek to prohibit the export of all computer source code regardless of content in order for the EAR/ITAR restraints to be content-neutral. This is not what these regulations do.

The *Karn* court held that the regulations are not content-based because the State Department is not regulating any expressive message contained on the disks. Explaining this rationale, the court noted that the government was not:

> regulating the export of the diskette because of the expressive content of the comments and or the source code, but instead [was] regulating [export of the diskette] 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.[203]

The court appears to have argued on the fact that disks were not expressive in the sense that they did not reflect a political sentiment or attempt to persuade the reader of anything. Because the disk's contents are purely instructional, the *Karn* court seemed to conclude that the contents are not expressive and therefore the regulations are not content-based. The Supreme Court expressly rejected the proposition, however, that a content-based regulation must restrict a particular viewpoint.[204]

Rather than support the contention that the ITAR restraints are content-neutral, this line of reasoning lends support to the notion that they are content-based. If the purpose of the regulation is to control potentially dangerous non-persuasive communications, as the *Karn* court appears to suggest, then the regulation, on its face, purports to regulate

[202] Letter notifying Karn of State Department decision to classify the Applied Cryptography diskette as a munition (visited Feb. 8, 1998) <http://people.qualcomm.com/karn/export/floppy_cjr_response.html>.

[203] Karn v. United States Dep't of State, 925 F. Supp. 1, 30 (D.D.C. 1996) (emphasis added).

[204] In a case concerning politically controversial publications, the Court cited FCC v. League of Women Voters of California, 468 U.S. 364, 383-84 (1984) in support of the proposition that "the First Amendment's hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic." Arkansas Writers' Project, Inc. v. Ragland, 481 U.S. 221, 230 (1987).

certain content. This is not to say that all content-based regulations are unconstitutional,[205] but rather that any regulation that probes content before determining applicability is content-based. Under the EAR/ITAR restraints, content is the determinative factor in deciding whether the petitioner may circulate the information abroad. The fact that the licensing scheme does not regulate persuasive or innocuous information illustrates the central role content plays in applying the regulation to would-be exporters. Furthermore, the argument that the EAR/ITAR restraints are content-based finds support in related case law.

In *United States v. Progressive, Inc.* and *New York Times Co. v. United States*, the government sought to enjoin the publication of certain information on the grounds that publication would harm national security.[206] In the face of those claims, the courts implicitly recognized that the injunctions sought by the government were content-based, noting that the restrictions came before the court with a heavy presumption against their validity.[207] Recall that restraints on expression that are content-based are presumptively invalid,[208] while restraints that are content-neutral will be subjected to a level of review akin to intermediate-level scrutiny.[209] From the presumed invalidity, one can infer that the courts operated on the belief that the restraints were content-based rather than content-neutral.

Likewise, the contents of the disk in *Karn* and the contents of the academic papers in *Bernstein* are the sources of contention in those cases. Just as it did in *Progressive* and *New York Times*, the Executive Branch in *Karn* and *Bernstein* alleges that publication of certain information will imperil national security.[210] Isolating certain information and then subjecting it to a governmental licensing scheme as done under the EAR/ITAR is plainly a restraint based on content.

[205] *See infra* Part III.D. for a discussion of permissible content-based restraints.

[206] United States v. Progressive Inc., 467 F. Supp. 990 (W.D. Wis. 1979) (information about hydrogen bomb construction); New York Times Co. v. United States, 403 U.S. 713 (1971) (information about United States' involvement in the bombing of Cambodia).

[207] *New York Times Co.*, 403 U.S. at 714; *Progressive Inc.*, 467 F. Supp. at 992.

[208] *See supra* note 191.

[209] *See, e.g.* United States v. O'Brien, 391 U.S. 367 (1968) (applying a least restrictive means test to a content-neutral law banning the burning of draft cards).

[210] The State Department's Memorandum of Points and Authorities in *Karn* stated the sources of the government's concern over permitting export of encryption. For an excerpt, see Karn, *Points & Authorities*, *supra* note 8

b. Review of Intent

Even though a finding that a regulation is content-based on its face is enough to create a presumption of invalidity, a review of the possible intent motivating the promulgation of the current encryption regulations is revealing. Some observers have argued that the regulations have the incidental and possibly intentional effect of chilling speech over electronic media and enabling the implementation of a domestic encryption policy without debate or public participation.[211] These allegations are explored in this Part.

In determining the rationale for the continuing regulation of encryption, the court should first look to the stated purpose of the regulation and assess how controlling that particular commodity supports the goal of the regulation. If the regulation does not appear to accord with the purpose of the Act, then the court should do more than scratch the surface to see if an ulterior motive exists.[212]

Congress announced the purpose of the AECA in the first subsection of the Act as "furtherance of world peace and the security and foreign policy of the United States."[213] The State Department included encryption technologies on the USML when it first promulgated the ITAR during the cold war in 1977. In doing so, it appears that the State Department was acting in furtherance of the stated goal of the AECA. The purpose of the EAA is generally to encourage exports from the United States, permitting the imposition of export controls only when they are necessary to protect national security, foreign policy, or supply objectives.[214] Any export controls promulgated under the authority of the EAA must "clearly further" one of these objectives.[215]

[211] *Whitehouse Off Base on Encryption Controls*, SEATTLE TIMES, July 18, 1996, at B4.

[212] Commenting on the need for judicial review, Chief Justice Marshall wrote, "[S]hould Congress, under the pretext of executing its powers, pass laws for the accomplishment of objectives not entrusted to the government . . . such an [enactment would not be] the law of the land." McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 423 (1819). Though Marshall's statement addressed Congressional acts, his reasoning seems equally applicable to the acts of administrative agencies, particularly when they are acting in a quasi-legislative (and certainly unforeseeable) capacity.

[213] 22 U.S.C. § 2778(a) (1994).

[214] 50 U.S.C. § 2402(2), (10) (1991 supp. 1997).

[215] *Id.*

President Clinton shifted control over dual-use encryption to the Commerce Department with reference to an earlier executive order promulgated in 1994.[216] This earlier executive order established a state of emergency arising from "unrestricted access of foreign parties" to certain American high technology goods and technical data.[217] Clinton concluded in the 1994 order that in order to deal with this problem of foreign access, the continuation of the EAA and the EAR would be necessary to protect the national security, foreign policy and the economy of the United States.[218] The 1996 Executive Order transferring control over encryption to the Commerce Department states that the transfer is being made as an additional remedial step to deal with the national emergency first declared in 1994. Thus, the stated purpose for the transfer of control over encryption to the Commerce Department is to protect national security.[219]

In 1977, encryption was used exclusively for military applications, enabling armies to communicate in code without fear of strategies being intercepted by the enemy. This fear of a diminution in foreign surveillance capabilities initially prompted the State Department to include encrypting technologies on the USML.[220] In including encryption technologies on the USML at that time, the State Department was acting in furtherance of the stated intent of the AECA.

However, in the nearly 20 years since the promulgation of the ITAR, strong encryption technology has spread far beyond the borders of the United States. Likewise, the uses of encryption have spread far beyond military applications.[221] The changes in the availability and use of encryption have seemingly frustrated the purpose of the AECA and the EAA with respect to controlling encrypting source code.

[216] President Clinton's order refers to Exec. Order No. 12924, 59 Fed. Reg. 43437 (1994). Clinton Order, *supra* note 50.

[217] Exec. Order No. 12924, 59 Fed. Reg. 43437 (1994).

[218] *Id.*

[219] This is justification is somewhat curious because the Commerce Department controls are marginally more relaxed than the State Department controls were. Most probably, the government made the transfer in order to loosen the controls over encryption somewhat, but did not wish to surrender its power to exercise full control, i.e. block all exports of encryption when it wished to. The declaration that the purpose of the transfer was related to national security may have the effect of keeping full control over encryption in the President's hands.

[220] Karn, *Points & Authorities*, *supra* note 8. If other nations' communications were encrypted, the United States would no longer be able to monitor activities inside foreign states. At the time that encryption technology was first banned from export, the State Department and the NSA shared the concern that permitting the export of high-grade encryption technology would enable foreign governments to encode their communications securely and foil our intelligence efforts.

[221] SCHNEIER, *supra* note 12, at xv.

PGP offers military-grade protection and is currently available outside the United States over the Internet free of charge.[222] Magazines and newspapers have reported widely on cases of foreign nationals using PGP to digitally cloak their criminal enterprises.[223] Furthermore, encrypting source code is also available abroad in print and can easily be converted into machine-readable code. Any sufficiently motivated individual could easily purchase a book, such as *Applied Cryptography*, that contains encrypting source codes and algorithms printed inside. With this information the person could then type or scan the contents into a computer. In a very short time, he or she could transform information available in print into fully functional military-grade encryption.

Any person who obtains a copy of a computer file in the United States can easily post the file on a computer for international distribution. This was done with the PGP program when Zimmerman, the inventor, gave copies away to friends in United States and the program found its way all across the globe.[224] The ease with which computer files can be transferred, copied, and made available over the Internet makes it difficult to believe that any valuable computer file located in the United States and widely available for domestic distribution will stay in the United States for any length of time. It is akin to saying that a secret printed in a nationally circulated newspaper will remain secret outside the United States after distribution.

Furthermore, the restraints in place in many applications designed to prevent unauthorized access or disclosure to foreign nationals appear ineffectual. These restraints typically take the form of requiring the user to accept certain restrictions as a condition of using the software. The user accepts by "clicking," after reading the terms, on a button labeled "I accept" at the bottom of the computer screen.[225] The reality is that

[222] *See supra* notes 33, 35.

[223] *See supra* note 35; *infra* note 294.

[224] *Government Drops Zimmerman PGP Prosecution*, NEWSBYTES NEWS NETWORK, Jan. 12, 1996, *available in* LEXIS, NEWS Library, PAPERS File.

[225] The following is the text of the terms and conditions of use presented to the user installing Netscape, a popular Web browser with built-in encrypting capabilities:

> Except for export to Canada for use in Canada, by Canadian citizens, the software and any underlying technology may not be exported outside of the United States or to any foreign entity or "foreign person" as defined by United States government regulations, including without limitations, anyone who is not a citizen, national or lawful permanent resident of the United States. By

users of computer software are routinely presented with terms and conditions of use and likely click "I accept" without ever reading the terms. These "agreements" are essentially digital contracts of adhesion equivalent to pages of fine print that make up today's widely used form contracts. Even the most diligent users are pressed to take the time to examine these agreements line-by-line. As a result, even well-meaning users may be unaware of the terms agreed to that prohibit distribution abroad.

Furthermore, no manageable controls are in place to prevent sending software over phone lines or carrying computer disks across borders in baggage. Based on the ease with which a person in the United States can send software abroad virtually instantaneously,[226] and considering the documented fact that military-grade encryption is already available outside the United States, it is doubtful that the regulation of encrypting source code substantially advances any purpose related to the stated goals of the AECA or the EAA.

Almost certainly, advances in microprocessor technology will, at some point in the future, make today's safest algorithms vulnerable to attack.[227] Let us say, for argument sake, that by the year 2020, cracking a 1248-bit PGP key will be possible in a reasonable amount of time. Let us also say that presently only three encrypting algorithms exist: PGP (maximum length key of 1248 bits), ABC (maximum length key of 1248 bits), and XYZ (maximum length key of 2000 bits).

At present, PGP is already widely available throughout the world while neither ABC nor XYZ is widely distributed. If PGP has no weaknesses or backdoors,[228] the earliest that the government can

> downloading or using the software, you are agreeing to the foregoing and you are warranting that you are not a "foreign person" or under the control of a foreign person.

Display at the end of the Netscape installation process (copy on file with author). Netscape's URL is <http://home.netscape.com/>.

[226] One Web site offers visitors the chance to engage in a bit of civil disobedience by pulling an encryption signature file into the United States from Anguilla and then re-exporting the file back out to Anguilla. This simple act violates encryption export regulations (visited April 2, 1997) <http://online.offshore.com.ai/arms-trafficker/>.

[227] *See supra* note 23. Commenting on IBM's newly announced "unbreakable" encryption scheme, one industry expert commented, "Just because something is unbreakable today doesn't mean it's going to be unbreakable in the year 2000." Ed Golden, *IBM Encryption Scheme Holds Significant Promise*, INFOWORLD, May 12, 1997, at 21.

[228] Zimmerman, inventor of PGP, has made the source code available for public inspection. It is regarded as the closest thing to military-grade encryption that is available in the public domain. SCHNEIER, *supra* note 12, at 437. A "backdoor" is a secret entrance, intentionally or accidentally created, that permits those aware of its existence to crack codes easily without going through the time and effort of a "brute force" attack. *See supra*, note 18.

expect to crack a PGP key is the year 2020. The same is true for ABC since it shares the same 1248-bit key length.[229] However, the government will not be able to crack XYZ with its longer key until some time after the year 2020.

In this scenario, efforts to control the export of either PGP or ABC would not serve to protect national security since PGP is already available internationally, is easily replicable, and because ABC offers no better protection than does PGP. However, regulation of XYZ, which is not already widely available, could serve to protect national security since it provides an additional period of security, during which XYZ-encrypted messages could be read. Applying this illustration to the facts of *Karn* and *Bernstein*, it follows that any efforts to control the export of encryption systems no stronger than PGP, or any of the algorithms already in circulation (for example, those in Part V of *Applied Cryptography*), do not serve to protect national security in any meaningful way.

Essentially, the genie has been let out of the bottle with the release of PGP, the publication of *Applied Cryptography*, and the spread of other encryption algorithms across the Internet. As a result, continuing to regulate the export of all encryption stronger than 40 bits (symmetric) does not serve to protect the nation's security. Those most likely to get caught in the web of these export restrictions are those least likely to pose a threat to the United States. Considering how easily one can obtain encrypting software over the Internet and how widely Internet users have distributed the program, it appears that any motivated person can obtain a copy of PGP anywhere in the world.[230]

Weighing the governmental interests, the realities of global access to encryption, and the increasing need for strong encryption on the Internet, a committee consisting of members of the National Research Council, the National Academy of Sciences and the National Academy of Engineering (the Committee) recently released a report calling for the freer use of encryption.[231] The report considered law enforcement and national security dilemmas posed by cryptography and concluded that "on balance, the advantages of more widespread use of cryptography

[229] If ABC has any weaknesses or previously unknown backdoors, it may be possible to crack the code much earlier than the year 2020.

[230] *See supra* note 35.

[231] Committee Recommendations, *supra* note 48.

outweigh the disadvantages."[232] Addressing the issue of export controls, the Committee found that because of its nature, it is difficult to monitor and control the export of software.[233] The Committee further found that as encryption proliferates, traditional monitoring of foreign parties' communications will become increasingly difficult.[234] Thus, the inexorable increase in use of encryption will substantially frustrate the government's ability to protect national security through encryption export regulations. The Committee's findings cast doubt on the wisdom of continuing to regulate encrypting software. They also make observers wonder about the real rationale for continuing to restrict source code exports.

Considering that military grade encryption is already available free of charge outside the United States and may be easily sent, albeit illegally, via phone lines or post to foreign nationals, continued regulation of encryption for the national security reasons seems futile. However, continuing the regulation of encryption may serve other purposes.

The EAR/ITAR regulations have had an impact on the strength of domestically available encryption.[235] Many popular word processors, spread sheets, and Internet "Web browsers" have built-in encrypting capabilities. The Committee found that restraints on encryption exportation have led many software manufacturers to save the cost of producing a high grade version for domestic use and a low grade version for export by simply producing one version compatible with the lowest common denominator.[236] The result has been that much of the commercial encryption available in the United States is weak.[237]

Since 1993, the Clinton Administration has tried to promulgate a national encryption standard which will preserve law enforcement's ability to wire tap and monitor electronic communications.[238] After two failed proposals, President Clinton has tried a third time to create a national encryption policy. Observers have dubbed this third proposal "Clipper III."[239] In the years since the first proposal, no market-led

[232] *Id.* at 6.

[233] *Id.* at 8.

[234] "In the long term, as the use of encryption grows worldwide, it is probable that national capability to conduct traditional signals intelligence against foreign parties will be diminished." *Id.*

[235] *See supra* notes 46, 48, 49 and accompanying text.

[236] *See supra* note 46 and accompanying text.

[237] *See generally* Charles L. Evans, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C.J. INT'L LAW & COM. REG. 469 (1994) (discussing the impact of the ITAR regulations on the U.S. software industry).

[238] *See supra* notes 38-45 and accompanying text.

[239] *See supra* notes 44-45 and accompanying text.

standard has emerged as the clear favorite.[240] This is not because the technology and the demand do not exist. It is the result of the software industry's inability to produce a single strong encryption standard for domestic and international sale. Additionally, for the sender and receiver to communicate, both must use the same encrypting algorithm. With the expansion of the Internet and electronic communications, users of the Internet are crossing borders with increasing frequency, communicating with the person next door one minute, exchanging ideas with someone on another continent the next. A strong encrypting program in use in the United States offers little or no protection when communicating with another using different or weaker technology. In short, the privacy offered by encryption is only as good as the weakest link in the chain of communication. The EAR/ITAR regulations have forged such a weak link.

By continuing to restrict the export of encrypting software, the Clinton Administration has essentially bought time for itself while it reworks its unpopular Clipper encryption system proposal. The regulation of encryption has had the incidental and possibly intentional effect of chilling speech and retarding the emergence of an international encryption standard. Considering the wide international availability of encryption, the continued regulation of encrypting source code that is already published and publicly available either in America or abroad fails to advance the stated purposes of the AECA or the EAA in any significant way.[241] Furthermore, it appears that the continuing regulation of encryption source code discourages citizens from communicating freely and transacting commercially over the Internet.[242] Effects of

[240] The DES, PGP, and RSA cryptosystems are the closest to being international standards for encryption. DES was considered the "worldwide standard" in 1994. SCHNEIER, *supra* note 12 at 219. RSA is thought to be the most popular public key cryptosystem in the world. SCHNEIER, *supra* note 12, at 281-82. For evidence of the worldwide popularity of PGP, see *supra* note 35. Nevertheless, licensing and export of these systems is restricted because all of them operate at more than 40 or 512 bits.

[241] Regulation of newly developed encryption that is stronger than that which is already available internationally would seem to advance the stated goals of the EAA and the AECA to protect and preserve national security.

[242] *Internet Commerce Hung up on Security*, 4 EDI NEWS, Feb. 19, 1996, *available in* LEXIS, MARKET Library, IACNEWS File.

these kinds strongly suggest an impact on speech that the Constitution does not permit.[243]

C. Availability of Judicial Review

Even if the EAR/ITAR regulations are otherwise valid content-based prior restraints working to protect national security, the regulations must provide a mechanism for prompt judicial review in order to make the prohibition of publication final.[244]

Both the ITAR and the EAR regulations purport, on their face, to permit no judicial review. The AECA expressly bars judicial review under the APA. The only remaining cause of action for the aggrieved exporter is to assert that her constitutional rights have been violated. Thus although the AECA does not provide a cause of action or a judicial review process, the Constitution ensures at least a minimal level of protection from the censor's pen.

The Export Administration Act of 1979 (EAA) provides for a greater level of judicial review than the AECA.[245] However, Executive Order 13,026 specifically exempts sections 4(c) and 6(h)(2)-(4) of the EAA.[246] The Order states that permitting judicial review could imperil national security and jeopardize "foreign policy interests."[247] Of course, this is ultimately an issue for a court to decide under the political question doctrine. However, neither the ITAR nor the EAR purport to provide a process for judicial review of the government's act of censorship. In fact, the Executive Branch has attempted to impose hurdles to judicial review by invoking the defense of national security.

In *Freedman v. Maryland*, the Court addressed a film licensing scheme that worked as a prior restraint, and required that procedural safeguards be implemented to ensure that the scheme did not run afoul of the First Amendment. The Court required that the government bear the burden of proof to justify the restraint, that the request for a license be handled in a brief period of time, and that the denial of a license should not become effective until the government agent seeking the restraint had gone to court and received an injunction.[248] In the case

[243] New York Times Co. v. United States, 403 U.S. 713, 714 (1971); United States v. Progressive, Inc., 467 F. Supp. 990, 992 (W.D. Wis. 1979).

[244] Blount v. Rizzi, 400 U.S. 410 (1971); Freedman v. Maryland, 380 U.S. 51 (1965); Hague v. C.I.O., 307 U.S. 496 (1939).

[245] The APA creates a presumption of a right to judicial review. This presumption can be overridden only by express language in a statute. *See supra* Part III.A.

[246] Clinton Order, *supra* note 50, at § 1.

[247] *Id.*

[248] *Freedman*, 380 U.S. at 58-59.

of a prior restraint and injunction barring the distribution of obscene printed materials, the Court held that the injunction would only be valid if similar procedural safeguards were in place.[249] Among the required safeguards was the right to prompt judicial review of the injunction.

Although the Maryland censorship law in *Freedman* provided for appeal to the state courts, the Court held that this process was too time consuming.[250] The Court expressed concern that as the aggrieved party sought judicial review in the state court system, the censor's determination, in practice, would become final.[251] To prevent this from happening, the Court required that any attempt at censorship be approved by a court shortly after the initial review. Expressing his concern over the censor's insensitivity toward the First Amendment, Justice Brennan wrote:

> [O]nly a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring judicial determination suffices to impose a valid final restraint. To this end, the exhibitor must be assured [that] the censor will, within a specified brief period, either issue a license or go to court to restrain showing the film. Any restraint imposed in advance of a final judgment determination on the merits must similarly be limited to preservation of the status quo for the shortest fixed period compatible with sound judicial resolution.[252]

Similar procedural safeguards should be implemented in the case of export licensing regulations. The danger of unchecked governmental censorship is just as great in the case of export licenses as it is in the case of film exhibition licenses. Like the Maryland statute in *Freedman*, the ITAR and EAR regulations do not provide for any sort of expedited judicial review before the licensing determinations become final. In fact, both regulatory schemes purport to prohibit all judicial review. In light of the requirement that speech licensing schemes must provide an avenue for prompt judicial review, it would seem that the EAR and ITAR schemes are facially unconstitutional.[253]

[249] Kingsley Books, Inc. v. Brown, 354 U.S. 436, 440-41 (1957).

[250] Freedman v. Maryland, 380 U.S. 51, 59-61 (1965).

[251] *Id.* at 58.

[252] *Id.*

[253] President Carter's Assistant Attorney General, John M. Harmon, came to a similar conclusion in a memorandum analyzing the constitutionality of the ITAR encryption regulations. Interestingly, at the time this memo was written, encryption had no commercial applications and was strictly of interest to mathematicians and spies. John M. Harmon, Assistant Attorney General, Office of Legal Counsel, *Constitutionality*

D. Countervailing National Security Concerns

Once a court has determined that source code is speech, and that the EAR/ITAR restraints are content-based, its next inquiry must be whether encrypting source code is protected speech. Although the First Amendment provides substantial protection for freedom of speech, it is well established that this right is not absolute.[254] Prior restraints are constitutionally permissible in certain instances.[255] In a 1931 decision that struck down a state prior restraint for libel, Chief Justice Hughes noted that, "[First Amendment] protection even as to a previous [prior] restraint is not absolutely unlimited."[256] Justice Hughes went on to articulate some of the "exceptional" cases in which a prior restraint would be permissible. These cases include utterances that hinder a country's war effort (such as publishing the number and location of troops), publishing obscene material, and publicly using words which incite violence.[257] The narrowly articulated instances led the Supreme Court later to coin the oft-repeated phrase in *Bantam Books v. Sullivan*, "[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."[258] Although the court in *Bantam Books* was addressing a Rhode Island statute regulating obscene and indecent publications, two years later the Court noted that its statement in *Bantam Books* applied as well to "other forms of expression." [259]

In specifically citing troop locations and military transport sailing dates as examples of information the expression of which the First Amendment does not protect, Justice Hughes carved out a class of speech not entitled to First Amendment protection: a class of speech consisting of words or utterances that imperil national security. Although Chief Justice Hughes' list was not meant to be exclusive, it suggests the severity and certainty of a threat that must exist for a prior restraint to be constitutional. Drawing from *Near v. Minnesota*, the

Under the First Amendment of ITAR Restrictions on Public Cryptography, May 11, 1978, *reprinted in* BUILDING IN BIG BROTHER, THE CRYPTOGRAPHIC POLICY DEBATE 543 (Lance J. Hoffman ed. 1994).

[254] *See e.g.*, Times Film Corp. v. Chicago, 365 U.S. 43, 47 (1961).

[255] Near v. Minnesota, 283 U.S. 697, 715-16 (1931).

[256] *Id.*

[257] *Id.* at 716.

[258] Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963); Freedman v. Maryland, 380 U.S. 51, 57 (1965); New York Times Co. v. Unites States, 403 U.S. 713, 714 (1971); Nebraska Press Ass'n v. Stuart, 423 U.S. 1319, 1324 (1975); R.A.V. v. St. Paul, 505 U.S. 377, 430 (1992).

[259] *Freedman*, 380 U.S. at 57.

Court in *United States v. New York Times* expounded on the degree of certainty that the government must demonstrate to support a prior restraint on speech.[260]

In a concurring opinion, Justice Brennan emphasized that the potential harm to national security posed by publication must be clear and certain, and cautioned that the First Amendment "tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result."[261] Justice Brennan further defined Chief Justice Hughes' requirement that publication would imperil national security:[262]

> [O]nly governmental allegation and *proof that publication must inevitably, directly, and immediately* cause the occurrence of an event kindred to imperiling the safety of a transport already at sea can support even the issuance of an interim restraining order. In no event may mere conclusions be sufficient.[263]

Thus, Brennan required that certain and demonstrable harm be inevitable to justify prohibiting publication of materials allegedly posing a threat to national security.

In 1979, eight years after the Supreme Court decided *New York Times*, the magazine *The Progressive* tried to publish technical information on the construction of the hydrogen bomb.[264] The article, entitled "The H-bomb Secret. How We Got It, Why We're Telling It," contained both information already in the public domain and information previously

[260] *New York Times Co.*, 403 U.S. at 713.

[261] *Id.* at 726.

[262] In *Near*, Justice Brennan noted that the cases thus far considered by the Court had indicated that a prior restraint is permissible only when the Nation is at war. *Id.* In the present case, the government may argue that the Nation is engaged in a war on terrorism, a war on drugs, or some other political hyperbole. Notwithstanding such rhetoric, the phrase "at war" appears to be a term of art in this context, referring to the state of war which can only be declared by Congress pursuant to Article I of the Constitution. U.S. Const. art. I, § 8. Any interpretation of the phrase less restrictive than this would permit the Executive Branch unilaterally to declare a national condition that could work to preempt certain civil liberties. The "war on drugs" provides a good example, having been waged for nearly 30 years. President Nixon first declared a "war on drugs" in 1969, and the Executive Branch's commitment to this "war" has since been actively reaffirmed by the Reagan, Bush and Clinton Administrations. Nevertheless, this state of "war" could not constitutionally justify abridgement of the due process rights of those accused of drug offenses.

[263] *New York Times Co.*, 403 U.S. at 726-27 (emphasis added).

[264] United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).

unavailable publicly.[265] After reviewing affidavits submitted by experts and scientists, the court found that publication of the article would pose a threat to national security.[266] One scientist appearing before the court stated that "the design and operational concepts described in the manuscript are not expressed or revealed in public literature nor . . . are they known to scientists not associated with the government weapons program."[267] Based on evidence presented at trial including statements of this sort, the court concluded that publishing the article would be analogous to publication of troop movements or transport sailing dates.[268] The *Progressive* court subsequently issued an injunction barring publication.[269]

In the case of exporting encrypting source code, the government has put forth nothing more than conjecture or surmise about the deleterious effects that it alleges will be wrought by electronic publication and distribution.[270] Considering that the cat is out of the bag with respect to the international availability of military-grade encryption, the State Department in *Karn* and *Bernstein* has not yet met the high burden of proof required by the Court under *New York Times*.

Publication and international distribution of the source code at issue in *Bernstein* and *Karn* would not result in the grave, immediate, direct and irreparable harm to the Nation required by Justice Brennan in *New York Times*. Because the book *Applied Cryptography* is already in wide circulation internationally, it is hard to imagine what harm is certain to befall the country if the codes found in the book were made available to the same readers in a different medium. Unlike the information on hydrogen bomb construction at issue in the *Progressive* case, the information in *Karn* has already been widely published and distributed.[271] In *Bernstein*, the government has offered no evidence that the source code at issue poses any threat to national security beyond that posed by PGP and equally strong encrypting applications published in *Applied Cryptography*.

The niche first carved out by Chief Justice Hughes and later defined by the Court in *New York Times* is a narrow one. Only information

[265] *Id.* at 992-93.

[266] *Id.* at 993-95.

[267] *Id.* at 992.

[268] *Id.* at 993.

[269] The injunction was later lifted after two other magazines published the information at issue in *The Progressive*. Eric B. Easton, *Closing the Barn Door After the Genie is Out of the Bag: Recognizing a "Futility Principle" in First Amendment Jurisprudence*, 45 DEPAUL L. REV. 1, 8 (1995).

[270] *See supra* note 8.

[271] Karn v. Unites States Dep't of State, 922 F. Supp. 1, 5 (D.D.C. 1996).

which will inevitably, directly and immediately imperil the Nation's security is denied First Amendment protection.[272] Although there was a time when publishing encrypting source code might have fallen within this narrow definition, international publication of source code currently presents no credible threat. In certain circles around the world, use of encryption is ubiquitous. If any of these groups or individuals presently want access to military-grade encryption, they need look no further than the Internet, their neighborhood library, local bookstore, or nearby software retailer. The release of equally strong encrypting source code does not pose a threat to national security sufficient to permit a prior restraint on publication. Encrypting source code should therefore be entitled to the protection of the First Amendment.

Determining that source code and encrypting applications are protected speech does not automatically mean that any regulations will be subject to strict scrutiny. The Court has afforded a lower degree of protection in the past to certain categories of speech. Offensive but not obscene speech, commercial speech, and speech in a labor context may be entitled to less protection than political, literary or scientific speech.[273]

Despite its economic applications, encryption is not commercial speech. A classic example of commercial speech is an advertisement for a business.[274] The mere fact that encryption source code is being printed and sold for a profit does not remove it from the realm of protected speech any more than the *Wall Street Journal* or a scientific textbook lose protection merely because they are printed and sold for a profit. For certain classes of people, encryption and source code is scientific speech. Such is the case for researchers and mathematicians like Mr. Bernstein. Most people, however, are not interested in the algorithms or source code driving the applications. From the end-user's

[272] New York Times Co. v. United States, 403 U.S. 713, 726-27 (1971).

[273] Some Supreme Court opinions seem to treat content-based regulations of speech differently depending on the nature of the speech subject to regulation. *See* LAWRENCE TRIBE, AMERICAN CONSTITUTIONAL LAW 2d Ed., (1988) § 12-18. Examples of cases drawing these distinctions include: FCC v. Pacifica Found., 438 U.S. 726 (1978) (offensive speech); Hoffman Estates v. Flipside, 455 U.S. 489 (1982) (commercial speech); Miller v. California, 413 U.S. 15, 24 (1973) (permitting regulation of obscenity but excluding literary, political, artistic, and scientific speech from the definition of "obscenity").

[274] Virginia State Bd. of Pharm. v. Virginia Citizens Consumer Council, 425 U.S. 748 (advertisement for prescription drug prices is commercial speech that is afforded some degree of constitutional protection).

perspective, encryption falls in neither a class of highly protected speech nor a class of less-protected speech. The Court may choose to create a new classification of speech for encryption aimed not at the academic, but at the end-user. However, if this is class is less protected, such a classification scheme raises the problem of a dual standard. A dual standard would be created because encryption is squarely within the classification of scientific speech for at least some readers. Such a dual standard might not only be difficult to administer, but might also make a regulation aimed at secrecy futile. The government may plug one hole in the dike, but another hole remains open and out of reach of government regulators.

In light of the findings that source code is speech, that the AECA/ITAR restraints are content based, and that the First Amendment protects encrypting source code because it poses no credible threat to national security, it appears that the government has acted unconstitutionally in denying Karn and Bernstein permission to export their wares. Buttressing this conclusion is an additional argument founded in the closely related futility doctrine.

E. The Futility Doctrine

Although the Supreme Court has never formally adopted nor expressly referred to the futility doctrine, at least one constitutional law scholar has found underpinnings of support for the doctrine in several landmark decisions.[275] Essentially, the futility doctrine states that "the First Amendment imposes a presumption against the [validity of any] suppression of speech when suppression would be futile."[276] A futile attempt to suppress exists when the information being suppressed is already available through another source and the purpose for the desired suppression is to preserve secrecy and prevent disclosure of the information. The futility doctrine applies only when efforts to suppress

[275] New York Times Co. v. United States, 403 U.S. 713 (1971); United States v. Progressive, Inc., 467 F. Supp. 990 (1979); Nebraska Press Ass'n v. Stewart, 423 U.S. 1319 (1975). For a complete discussion of the futility doctrine in First Amendment case law, see generally Easton, *supra* note 269.

[276] Easton, *supra* note 269, at 6. One might argue that adopting the futility doctrine would create an incentive to break the law, because individuals could trigger the application of the doctrine simply by disclosing the secret information. Once disclosed and in the public domain, further disclosure of the information would be entitled to the protection of the doctrine. However, this reasoning ignores the disincentives to be the first to disclose. Congress has made it a crime to disclose information listed on the USML. Those who dare to disclose initially still face criminal prosecution for taking the information public. The futility doctrine protects those who wish to make use of the information that is already in the public domain but doctrine offers nothing to those who disclose hitherto secret information.

would be ineffectual. Thus, it would not apply to regulations designed to suppress "fighting words" merely because another once uttered the words.[277] In such a case, continued regulation is not without effect. It may be expected to prevent future disturbances of the peace. Additionally, the purpose of the regulation is not related to preserving secrecy. Where the issue is the preservation of secrecy, however, once someone has revealed and widely distributed the secret, any future regulations suppressing that speech would be futile. The idea of prohibiting futile restraints on speech has found some support in First Amendment case law.[278]

Two concurring opinions and one dissenting opinion in *New York Times v. United States* alluded to the futility doctrine.[279] Justice Douglas' concurring opinion noted that the government sought to enjoin publication of information that the New York Times had already distributed.[280] Justice White made the same observation and went on to question the efficacy of an injunction once the information had already been leaked.[281] In stating that the petition for injunction came too late, the Justices focussed on the futility of prohibiting an act already committed.[282]

In *United States v. Progressive, Inc.*, the government withdrew its injunction barring *The Progressive* from publishing information about how to make a hydrogen bomb once two other publishers had made the

[277] Other classes of speech that would not be protected under the futility doctrine include advocacy of lawless conduct, libel or slander, fraudulent misrepresentation, and obscenity.

[278] *See supra* note 275. In another case significant for the scope of the 14th Amendment's protection of "liberty," Justice Harlan wrote, "This 'liberty' is not a series of isolated points pricked out in terms of the taking of property; the freedom of speech, press . . . and so on. It is a rational continuum which, broadly speaking, includes a *freedom from all . . . purposeless restraints*." "The Fifth Amendment protection on 'liberty' applies to the federal government and would presumably be no narrower that the interests protected by the 14th." Poe v. Ullman, 367 U.S. 497, 543 (Harlan, J., dissenting) (emphasis added).

[279] *New York Times Co.*, 403 U.S. 713 (Douglas, J., concurring, White, J., concurring, and Harlan, J., dissenting).

[280] *Id.* at 723 n.3 (Douglas, J., concurring).

[281] "So here, publication has already begun and a substantial part of the threatened damage has already occurred. . . access to the documents by many unauthorized people is undeniable, and the efficacy of equitable relief against these or other newspapers to avert anticipated damage is doubtful at best." *Id.* at 733 (White, J., concurring).

[282] Easton, *supra* note 269, at 8.

information available to the public.[283] Presumably, the government attorneys recognized the futility of barring the publication of information that was already available to the same audience via another source.

In dealing with the issue of exportation of encryption, the futility doctrine presents a compelling case. Strong encryption algorithms are already widely available throughout the world, either in source code found on computer disks, as downloadable files on the Internet, or in books found at local libraries and bookstores. Additionally, the current regulatory scheme seems to permit American companies to sell strong encryption through their partially-owned subsidiaries located abroad.[284] A circuitous distribution scheme like this does not appear to violate EAR or ITAR so long as the parent does not directly supply the technology to the subsidiary. There are number of ways for a corporate parent to effect distribution without violating the letter of ITAR or EAR.[285]

Acknowledging the ineffectiveness of export controls that attempt to regulate widely available technology, Congress expressly required that the President not impose export controls under the EAA where the technology was already widely available abroad.[286] Additionally, Congress has qualified the President's power to impose export restrictions by limiting the controls to those which the government has the ability to enforce effectively.[287] Together, these statutory limits on the Executive power to govern exports are evidence of Congress' concern that regulations not be ineffective or unenforceable. These are the same concerns that underpin the futility doctrine.

[283] *Id.*

[284] Sun Microsystems is the first American company to test these waters. Sun announced that it will sell 128-bit encryption through a partially-owned Russian subsidiary called Elvis+ Co. The encryption to be sold through Elvis+ uses triple DES and other algorithms. David Bank, *Sun's Selling of Encryption to Skirt Policy*, WALL ST. J., May 19, 1997, at A3. By incorporating a subsidiary in a foreign country and then creating an Internet storefront on a server located within the boundaries of that nation, an American company might be able to use the Internet as a distribution mechanism without technically running afoul of the EAR or ITAR.

[285] IDEA, a 128-bit cipher that was authored in Europe, is one example of very secure encryption created abroad that could be legally distributed through a partially or wholly-owned subsidiary of a U.S. company so long as the subsidiary was located outside of the United States. U.S. parent corporations could also purchase licenses for their foreign subsidiaries to use strong U.S. or foreign-source encryption so long as the licensor is located outside the United States. Because ITAR and EAR do not restrict the import of strong encryption, a parent and foreign subsidiary could communicate with secure encryption without violating either regulatory scheme.

[286] 50 U.S.C. § 2403(c).

[287] 50 U.S.C. § 2405(b)(1)(E). Considering how easily encryption source code and software can delivered over the Internet and through e-mail, it would seem that this provision of the EAA could never be satisfied with respect to the regulation of encryption exports.

Applying the futility doctrine to the facts of *Bernstein* and *Karn*, it is clear that little is accomplished by preventing the export of the diskettes containing the same information as contained in the approved-for-export book, *Applied Cryptography*, and Bernstein's approved-for-export academic papers. Readers of these materials can easily type or scan the source codes contained in print onto a computer diskette, yielding virtually the same product that the government banned from export.[288]

IV. CONCLUSION

Courts faced with petitioners seeking to export encrypting software or source code have two related doctrines from which they can draw guidance. The first is the prior restraint analysis,[289] predicated on a finding that source code is speech and that the EAR/ITAR regulations are content-based. Closely related to the final question under the prior restraint analysis of whether the source code is protected speech is the futility doctrine, drawn from dicta taken from several landmark restraint-of-speech decisions.

The analysis of the constitutional issues raised in *Karn* and *Bernstein* reveals that the EAR/ITAR licensing restrictions are both ineffectual in advancing the goal of national security and an unconstitutional infringement on the freedom of speech. In light of these findings, courts faced with challenges to encryption export regulations governing source code no stronger than that which is already available abroad, should strike down the regulations as unconstitutional and permit the petitioners to publish and distribute their information abroad.[290]

Many experts agree that the proliferation of encryption technology is in the best interest of the country.[291] At present, parties living in the United States with an interest in encrypting software have legal access to strong encryption. However, as discussed above, these same parties may not distribute copies of the software to friends and colleagues abroad without first applying for a license from the government. This

[288] Karn v. United States Dep't of State, 925 F. Supp. 1, 1-3 (D.D.C. 1996).

[289] *See supra* Parts III.A.-III.D.

[290] Although the USML restricts both encrypting software and hardware, the facts surrounding the regulation of software and source code should not be confused with the facts surrounding the regulation of encrypting hardware or other items listed on the USML. Each case needs to be analyzed on its merits.

[291] *See supra* notes 231-44 and accompanying text.

poses a problem because many domestic users of encryption do not have the same encrypting programs as their foreign colleagues, making compatibility an issue for communicating in secret both internationally and domestically. Presumably, the easiest way to resolve the problem of incompatible encryption systems is to establish a communications protocol beforehand and share common encrypting software between parties who anticipate a need to communicate in private.

The EAR/ITAR regulations prohibit establishing such a protocol internationally if the parties wish to use strong encryption. Law-abiding citizens are left without secure means to communicate in secret across international borders while those who disregard the law freely exchange software and source code internationally.[292] As a result, networks of criminals can place their communications beyond the reach of law enforcement while law-abiding citizens' communications remain accessible.[293] Presumably, law enforcement officials have no legitimate reason to monitor the communications of law-abiding citizens, yet increasingly these are the only people whose communications remain intelligible to law enforcement and third party eavesdroppers. In short, the additional harm which may be wrought by legalizing the international distribution of encrypting source code is minimal while the benefits to be gained are significant.

Newspapers and magazines have reported widely on the need for increased privacy and security over the Internet and the chilling effect on speech created by the current lack of privacy.[294] These reports deal primarily with commercial applications, but apply to noncommercial speech as well. Although sending a letter via e-mail may be easier, cheaper and more efficient, concerns about privacy may incline one not to choose e-mail.[295] Alternative forms of communication are available,

[292] *See supra* note 35.

[293] A group of pedophiles has published a collection of pornographic photographs over the Internet in Europe, using encryption to evade detection by the police. Thomas Sancton, *Preying on the Young all Over the World, Boys and Girls are Abused in a Vicious Sex Trade Now Abetted by Computer Networks*, TIME, Sept. 2, 1996, at 22.

[294] A simple search performed February 9, 1998 in LEXIS/NEXIS for the key words "Internet," and "privacy," or "security" revealed 32,425 stories fitting the search parameters. (search term "atleast 2(Internet) and (privacy or security)" *in* NEWS Library, PAPERS File).

[295] Commenting on the ease with which third parties can intercept and read others' e-mail, one scholar wrote, "Far from preserving our anonymity, the Web makes us far more exposed . . . the more we use machines like telephones and computers for communicating, the more we're susceptible to surveillance. If you want to remain anonymous, you have to go lo-tech." Rodan, *supra* note 2, at 4. Arguably, the only alternative to "going lo-tech" is to secure communications with strong encryption.

but none are as fast or potentially economical as electronic media.[296] However, concerns about privacy may stifle the continued growth and use of the Internet. With the proliferation of encryption, privacy concerns vanish. The emergence and growth of the Internet presents previously unimagined opportunities for communication and the sharing of ideas and data. However, just as people act with discretion and limit what they talk about with others in public places, users of the Internet must do the same.

In the days of the Framers, parties wishing to talk in private could simply select a discrete location and rest assured that no one could eavesdrop on their conversation. Today, slipping away to a discrete location when communicating across great distances is impossible. Encryption enables us to do today across great distances what has been possible to do for millennia only in close proximity. In this sense, encryption is the equivalent of a digital whisper.

Concerns about privacy and unauthorized access to our private transactions are slowing the development of the Internet and chilling electronic speech. Some have implemented ineffectual stopgap measures to discourage those with prying eyes, while others simply forgo communicating across electronic media when particularly concerned about privacy. In all, we have not come close to realizing the full potential of the Electronic Information Age. To do so, encryption is essential.[297]

However, the retarded growth of electronic privacy is not due to an unsolvable technical problem. Rather, it appears to be due to a

[296] Like telephone conversations and facsimile transmissions, e-mail communications can be conducted nearly instantaneously. In addition, once an e-mail account is set up, one can send messages to other e-mail users anywhere in the world for the cost of a local telephone call - essentially no additional cost to most users. For information on the benefits of using e-mail in a legal practice, see Charles R. Merrill, *Lawyers Push the E-Mail Envelope*, NEW JERSEY LAW J., Apr. 26, 1993, at 20.

Note, however, that by sending confidential messages via e-mail, the attorney-client privilege may be considered to have been waived. As encryption becomes increasingly prolific, and as reports of computer surveillance and electronic espionage continue to surface, it is foreseeable that failure to encrypt could prove in the near future to be grounds for a negligence cause of action. One legal publisher recently released guidelines for use of e-mail and how to avoid liability for, among other things, negligent disclosure. *Tech Notes*, CORP. LEGAL TIMES, June 1996, at 55. *See also* Marcelo Halvern, *Attorney-Client Privilege in the Internet Age*, 1 INTERNET NEWSLETTER: LEGAL AND BUSINESS ASPECTS, July 1996, at 12.

[297] Friedman, *supra* note 17, at 223.

governmental policy begun during the Cold War. The policy has survived to this day relatively unscathed through either sheer sclerosis or by design, allowing the government continued access to domestic and international communications. President Clinton's recent reshuffling of the encryption export controls shows that the Executive Branch is aware of the need for more liberal controls over this important communication tool. However, it is almost certain that the current Administration fears that widespread use of encryption will foil international and domestic criminal investigations. Working to prevent this evil, the Administration has thrown up a roadblock in the path of encryption proliferation in the form of export regulations. The proper tool for such a policy is Congressional action.[298]

Regardless of the government's actual intent, restraints like those implemented through ITAR, EAR and any other similarly fashioned regulation are unconstitutional. These regulations, though driven by arguably laudable goals, have sought to achieve their ends by suppressing the circulation of protected speech. The choice between suppressing information or dealing with the dangers of its publication and potential misuse is ultimately made for us by the First Amendment.[299]

RYAN ALAN MURR

[298] Presently, the Congress is considering two bills that would drastically change the current regulatory framework: *Security and Freedom through Encryption Act (SAFE),* H.R. 695 105 Cong. 1st Sess.; *Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997,* S.B. 1726, 104th Cong. 2d Sess., reintroduced as S.B. 377, 105th Cong. 1st Sess. These bills would liberalize export controls, although to differing degrees. Proposed amendments may significantly alter their shape and effect, however, amendments proposed by Mike Oxley (R-OH) and Thomas Manton (D-NY) would provide immediate law enforcement access to private online communications and business transactions, prohibit the domestic manufacture, sale, import, and distribution of encryption that did not offer law enforcement access, and permit the Attorney General to set software standards and Internet service provider standards to ensure access for law enforcement.

For more information about these bills, including text of the bills and analysis, see:
(last modified Nov. 5, 1997) <http://www.cdt.org/crypto/>;
(visited Feb. 8, 1998) <http://www.crypto.com/safe_bill>;
(visited Feb. 8, 1998) <http://www.crypto.com/procode/>.

[299] Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 770 (1976).