DePaul University
UNIVERSITY LIBRARIES

DePaul Law Review

Volume 48
Issue 2 *Winter 1998: Symposium - The American Civil Jury: Illusion and Reality*

Article 18

A Constitutional Challenge to Encryption Export Regulations: Software Is Speechless

Yvonne C. Ocrant

Recommended Citation
Yvonne C. Ocrant, *A Constitutional Challenge to Encryption Export Regulations: Software Is Speechless*, 48 DePaul L. Rev. 503 (1998)
Available at: https://via.library.depaul.edu/law-review/vol48/iss2/18

A CONSTITUTIONAL CHALLENGE TO ENCRYPTION EXPORT REGULATIONS: SOFTWARE IS SPEECHLESS

INTRODUCTION

> The world isn't run by weapons any more, or energy or money; it's run by little ones and zeros, little bits of data. It's all just electrons . . . there's a war out there old friend, a world war, and it's not about who's got the most bullets; it's about who controls the information, what we see and hear, how we work, what we think; it's all about the information.[1]

Historically, governments throughout the world used encryption technology to protect military secrets.[2] Today such software has evolved into an invaluable tool for individuals and businesses requiring "authenticity, confidentiality, and integrity of electronic communications and transactions"[3] on the Internet.[4] While the government is concerned with ensuring public safety, individuals and businesses are concerned with protecting proprietary or confidential information, ex-

[1] SNEAKERS (Universal 1992).

[2] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C xv (1994) ("For many years, . . . cryptography was the exclusive domain of the military."); Marcia S. Smith, *Encryption Technology: Congressional Issues*, CRS ISSUE BRIEF (Cong. Res. Serv.), Oct. 20, 1997, at 1, 1; J. Terrence Stender, Note, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 CASE W. RES. J. INT'L L. 287, 289 (1998) ("Typically, emphasis has been on the protection of state or military secrets and, of course, the collection and exploitation of adversaries' secrets.") (footnote omitted); *see* HARRY HOWE RANSOM, CENTRAL INTELLIGENCE AND NATIONAL SECURITY 116 (1959) ("Problems as old as intelligence itself are the secure communicating of secret information and the interception of such information transmitted by foreign governments or their espionage agents. The use of professional code makers and code breakers is perhaps as old as diplomacy and espionage."); Richard Raysman & Peter Brown, *The Continuing Debate Over Encryption Software*, 220 N.Y. L.J. 3, 3 (1998), *available in* LEXIS, Legal News Library, NYLAWJ File ("At one time, encryption technology was only used by the military and the government to protect state secrets as well as to access private information held by others.").

[3] Raysman & Brown, *supra* note 2, at 3. "During the last twenty years, there has been an explosion of public academic research in cryptography. For the first time, state-of-the-art computer cryptography is being practiced outside the secured walls of the military agencies." SCHNEIER, *supra* note 2, at xv; *see* Stender, *supra* note 2, at 289 ("[W]ith the rapid advances in computer technology over the last fifty years and the new vulnerability that technology has brought with it, encryption technology has become a valued tool for both businesses and individuals in the protection of proprietary and personal information.").

[4] *See* Raysman & Brown, *supra* note 2, at 3; *see also* Stender, *supra* note 2, at 288, 290 ("[The] interests, whether it be government, business or individual, . . . are not necessarily at odds . . . . Secure communications, secure data storage, individual privacy and a robust economy are with little doubt within the most basic national interest.").

ploiting a potentially profitable technology, and preserving the constitutional right to privacy and freedom of speech.[5] In an attempt to satisfy the burden of protecting public safety, the government has placed national security controls on the export of encryption technology.[6] These controls are continuously challenged as, among other things, a violation of individual freedom of speech.[7]

Two recent cases encapsulate this First Amendment debate. In *Bernstein v. United States Department of State*,[8] Judge Marilyn Patel ruled that the new export regulations violated the First Amendment as a prior restraint on speech.[9] In a prior decision, Judge Charles R. Richey, in *Karn v. United States Department of State*,[10] found the software source code and the author's written comments speech protected by the First Amendment. Applying the *O'Brien* test,[11] however, the court found the government regulation was justified, as it was narrowly tailored to the goal of limiting the proliferation of cryptographic products.[12]

Part I of this Comment provides a background of software and cryptography.[13] Part II details the government regulations and policies controlling the export of cryptographic technology.[14] Part III dis-

[5] *See* Sean M. Flynn, *A Puzzle Even The Codebreakers Have Trouble Solving: A Clash of Interests Over The Electronic Encryption Standard*, 27 LAW & POL'Y INT'L BUS. 217, 218 (1995); *see also* Stender, *supra* note 2, at 320.

> There is little question that enormous advances in telecommunications in the fifty years have created the opportunity for public use of encryption to ensure the privacy and integrity of business and personal communications. However, at the same time, these same advances seriously threaten the capabilities of law enforcement and intelligence agencies to intercept a broad range of signal intelligence targets, for instance, narcotraffickers, organized crime, terrorists, and foreign espionage agents. Diverse interests are in diametric opposition to each other: industry's right to sell and the public's right to use crypto versus the government's duty to protect.

Id. (footnotes omitted); *see* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and The Constitution*, 143 U. PA. L. REV. 709, 718-34 (1995) (presenting examples of society's need for encryption technology to protect communications and provide data security today and in the future). The list of interested parties and their respective concerns are not all inclusive. The list merely serves to introduce the players and conflicting interests relevant to the focus of this Comment. The privacy and commercial profitability debates are beyond the scope of this Comment.

[6] *See infra* Part II.

[7] The export regulations have also been challenged as an obstacle to commercial profitability. "[G]overnmental policy regulating this technology is beginning to pose some very serious commercial concerns." Stender, *supra* note 2, at 320.

[8] 974 F. Supp. 1288 (N.D. Cal. 1997).

[9] *Id.* at 1308.

[10] 925 F. Supp. 1 (D.D.C. 1996).

[11] *See infra* Part III.E.

[12] *Karn*, 925 F. Supp. at 12.

[13] *See infra* Part I.

[14] *See infra* Part II.

cusses Supreme Court guidelines for interpreting what speech is protected under the First Amendment.[15] Part IV examines the *Bernstein* and *Karn* encryption opinions regarding government export controls on data-scrambling software under the confines of the First Amendment.[16] Part V presents a First Amendment analysis of encryption source code as protected speech.[17] Specifically, this section first argues that encryption software is not speech. Second, Part V proposes that even if software is speech, software is not speech protected by the First Amendment. Finally, Part V suggests that even if software is speech protected under the First Amendment, software is expressive conduct and thus is afforded limited First Amendment protection. Part VI suggests the impact of case precedent and proposed legislation on future lawsuits.[18] Part VII concludes that the First Amendment does not prohibit government export controls on encryption software.[19]

I. Technology

A. Software

> We do not need to have an infinity of different machines doing different jobs. A single one will suffice. The engineering problem of producing various machines for various jobs is replaced by the office work of 'programming' the universal machine to do these jobs.[20]

Software consists of programs that enable a computer to function as multiple computers with various capabilities.[21] Interestingly, the genesis of computer technology did not utilize computer programs as a means of operation.[22] The computer would be wired by hand to perform one task at a time.[23] When a different task was desired, computer engineers were required to rewire the machine, consequentially causing many days of computer downtime.[24] The development of pro-

[15] *See infra* Part III.

[16] *See infra* Part IV.

[17] *See infra* Part V.

[18] *See infra* Part VI.

[19] *See infra* Part VII.

[20] Andrew Hodges, Alan Turing: The Enigma 293 (1983).

[21] Pamela Samuelson, *Contu Revisited: The Case Against Copyright Protection For Computer Programs In Machine-Readable Form*, 1984 Duke L.J. 663, 679-81.

[22] *Id.* at 673-74.

[23] *Id.* at 674.

[24] *Id.* at 674 n.33; *see id.* at 674. The first electronic computer developed in 1945, called the Electronic Numerical Integrator and Calculator ("ENIAC"), performed its functions one at a time in a prescribed order. *Id.* For each different operation, "ENIAC had to be manually rewired, like an old wire-and-plug telephone switch board, a task that could take several days." *Id.* at 674 n.33 (citing Frederic Golden, *Big Dimwits and Little Geniuses*, Time, Jan. 3, 1983, at 30).

grams, therefore, was a major breakthrough in the evolution of the computer.[25] Computers were able to store and use programs to perform particular tasks, thereby eliminating the need for hardware modifications every time an additional task was desired.[26] One of the most significant results of this development was that computers became "universal machines."[27] In other words, a computer could perform any task capable of being broken down into program instructions.[28]

Software programs are developed to run a process or perform a function.[29] "Software is that which empowers a computer to handle

[25] *See* Samuelson, *supra* note 21, at 674 ("An important development in the history of computers was that a computer could be made to store and use encoded instructions, 'programs,' to perform particular tasks, thus eliminating the necessity for making modifications to the hardware of the machine to change the tasks that it could perform.") (footnote omitted).

> It is possible to construct a customized piece of hardware to do any given task that might otherwise be programmed on a universal machine. A completely hardwired machine may do that given task more rapidly than a programmed computer. The prime advantage of the programmable computer is its generality. That is, it does away with the need to construct many different kinds of machines because one machine can be built and programmed to perform a variety of functions. Another of the implications of the development of programmable computers is that such computers were built so that the hardware itself could no longer perform any useful function without the directions given to it by a computer program.

Id. at 675; *see* Hoo-Min D. Toong & Amar Gupta, *Personal Computers*, Sci. Am., Dec. 1982, at 87, 88 ("The hardware can do nothing by itself; it requires the array of programs, or instructions, collectively called software.").

[26] Samuelson, *supra* note 21, at 674 (citing David A. Patterson, *Microprogramming*, Sci. Am., Mar. 1983, at 50, 52) ("The principle of the stored program, the invention of which was a milestone in the development of the modern digital computer, makes it possible to change the function of a computer by changing the contents of its memory unit instead of by changing its hardware.").

[27] *Id.* (defining universal machines as "machines capable of performing any task for which it was possible to create program instructions").

> It is possible to construct a customized piece of hardware to do any given task that might otherwise be programmed on a universal machine. . . . The prime advantage of the programmable computer is its generality. That is, it does away with the need to construct many different kinds of machines because one machine can be built and programmed to perform a variety of functions.

Id. at 675.

[28] *Id.* at 674; *see, e.g.*, Hodges, *supra* note 20, at 318-21; *see also* Samuelson, *supra* note 21, at 675 n.36 ("While many modern computers are programmed to perform only one function—running the watch you wear on your wrist, for instance—they may be capable of being programmed to do any number of different things.").

[29] *See* Samuelson, *supra* note 21, at 676.

> Properly programmed, the hardware can perform the series of steps necessary to accomplish a task as directed by the program.
>
> One could say that the set of instructions which constitutes a computer program gives the machine the "knowledge" it needs to do the task, but this is using the word "knowledge" in a very different sense from that in which it is normally used. A more accurate way to describe a program would be to say that the program's instructions simply prescribe an order for the hardware's execution of its primitive functions. This is, at base, the definition of a program.

information and to control information flow."[30] Additionally, others have defined software as a machine with both a program in passive text and a program capable of active execution.[31] When a computer programmer designs a system to perform a specific function or functions, he or she must then build the actual computer code that will make up the components enabling the system to operate.[32] Other than special purpose components, the program is written in what is known as "source code."[33]

Source code, the passive text, is a high level code[34] that presents a precise set of operating instructions enabling a computer to perform specific functions.[35] This code may also include comments written by the programmer describing what the code is about.[36] A computer, however, does not directly read source code.[37] Commercially available software compiles the source code instructions into "object code," also referred to as "machine" level code,[38] written in zeros and ones.[39] This code is read by the computer, enabling it to perform the specified functions.[40]

The principle function of source code is to provide a compiler with sufficient information to produce an "executable" computer pro-

Id.

[30] Gregory A. Stobbs, Software Patents 50 (1995).

[31] David Gelernter & Suresh Jagannathan, Programming Linguistics 1, 1-2 (1990).

> The program text represents the machine before it has been turned on. The executing program represents the powered-up machine in active operation. There is no fundamental distinction between the passive program text and the active executing program, just as there is none between a machine before and after it is turned on.

Id. at 2.

[32] Stobbs, *supra* note 30, at 66.

[33] *Id.* Programmers who write source code have a variety of computer languages to choose from. The programmer selects a particular language because it is most efficient and effective for the required function of the finished software, or the client for whom the software is being developed requested a specific language be used, or simply because it is the form which the developer is most familiar. *Id.*

[34] Encyclopedia of Computer Science 1263-64 (Anthony Ralston & Edwin D. Reilly eds., 3d ed. 1993).

[35] *See* Samuelson, *supra* note 21, at 680. See *supra* notes 28-29 and accompanying text for a discussion of the function software provides.

[36] Stobbs, *supra* note 30, at 170.

[37] *Id.* at 68.

[38] Peter D. Junger, Computers and the Law 12 (1996); Samuelson, *supra* note 21, at 683.

[39] Stobbs, *supra* note 30, at 68. This form is also known as binary code. *Id.*

[40] *See id.* at 171 (summarizing the function of source code as a "list of instructions, written in a selected computer language, and then converted into computer machine language, which the computer uses to build the software machine described by the instructions . . . the source code is simply a detailed blueprint telling the computer how to assemble those components into the software machine").

gram.[41] The users of the programs, for the most part, do not care what the software says to the computer.[42] Furthermore, the code written by the developer is not easily read by even the most experienced programmers.[43] For that reason, patent attorneys are advised not to rely on source code for an understanding of the program.[44] "Even with well-documented comments, one person's source code can be difficult for another person to read and comprehend. Therefore, it is best not to rely entirely on source code in describing a software invention in the specification."[45] Deciphering someone else's source code is an extremely time-consuming task,[46] and therefore the function of various source codes can be found written in textbooks and other printed media.

B. Cryptography

A cryptographic[47] program is commonly used software that has two basic functions: encoding (or encryption) and decoding (or decryption).[48] Encryption source code is defined as "a precise set of operating instructions to a computer that, when compiled, allows for the execution of an encryption function on a computer."[49] Encryption object code is defined as "computer programs containing an encryption source code that has been compiled into a form of code that can be directly executed by a computer to perform an encryption function."[50] The encryption process converts a readable message, artfully known as "plaintext,"[51] into unintelligible data traditionally known as "ciphertext."[52] The program then decodes the "ciphertext" back into

[41] *Id.* at 170.

[42] Samuelson, *supra* note 21, at 682. "The user does not care how the program does what it does, just that it does what it is supposed to do." *Id.* Notably, a program's object code may be the only form of the code available in the market. "[O]nce the program is operating correctly, the source code becomes superfluous. Only the machine-readable version is generally distributed." *Id.* at 681-82 n.67.

[43] STOBBS, *supra* note 30, at 240 (describing the process of deciphering someone else's source code as a time-consuming undertaking).

[44] *Id.* at 170, 240.

[45] *Id.* at 170.

[46] *Id.* at 240.

[47] SCHNEIER, *supra* note 2, at 1 (defining cryptography as "[t]he art and science of keeping messages secure" and encryption as "[t]he process of disguising a message in such a way as to hide its substance").

[48] Lance Hoffman, *Cryptography: Policy and Technology Trends* (visited Oct. 16, 1997) <http://www.eff.org/pub/Privacy/crypto-policydoe94.report>.

[49] 61 Fed. Reg. 68,585, 68,585 (1997) (to be codified at 15 C.F.R. pt. 772).

[50] *Id.*

[51] SCHNEIER, *supra* note 2, at 1; 61 Fed. Reg. at 68,585.

[52] Smith, *supra* note 2, at 1; *see* SCHNEIER, *supra* note 2, at 1 (defining an encrypted message as ciphertext).

"plaintext" through the process of decryption.[53] The encryption and decryption functions are made possible by compatible "keys."[54] These keys are a sequence of bits[55] which act as passwords and are given to both the sender and receiver of the message so that the text may be encrypted and decrypted.[56] The keys ensure that the sender and receiver are actually who they claim to be.[57] The longer the sequence, the more difficult the message is to break without the compatible key.[58]

II. Regulatory Background

A. *Prior Regulatory Framework*

The International Traffic In Arms Regulations ("ITAR") implemented the Arms Export Control Act ("AECA"), which in turn sets forth the United States Munitions List ("USML").[59] Part 121 of the ITAR presents the USML, which defines those items to be designated as "defense articles."[60] Congress enacted the AECA in response to

[53] Schneier, *supra* note 2, at 1.

[54] Smith, *supra* note 2, at 1.

[55] Bits is short for "binary digits." *See* John Bylinsky, *The Next Battle in Memory Chips*, Fortune, May 16, 1983, at 152.

[56] Smith, *supra* note 2, at 1. One author offered a simple hypothetical facilitating an understanding of the relationship between the stages of cryptography:

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

Jason Kerben, *The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Genie*, 5 Comm. Law Conspectus 125, 125 (1997).

[57] For example, in the hypothetical in note 56, the keys will ensure that Ruth is the receiver as Sam intended and Sam is the sender as Ruth intended.

[58] "[T]he sizes of encryption keys are measured in bits and the difficulty of trying all possible keys grows exponentially with the number of bits used. Adding one bit to the key doubles the number of possible keys; adding ten increases it by a factor of more than a thousand." Matt Blaze, *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security* (visited Oct. 15, 1997) <http://www.cdt.org/crypto/>.

[59] 22 C.F.R. pt. 121 (1998).

[60] *Id.* § 121.1 Category XIII(b)(1). The ITAR refers to "technical data" as an item subject to the licensing requirement. Technical data is information "which is required for the design[,] development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles." 22 C.F.R. § 120.10(a)(1) (1996), *revised by* 61 Fed. Reg. 48,831 (1996). However, technical data, for purposes of the ITAR, that are deemed to be in the public domain, are not subject to the restriction. *See id.* § 120.11. If information is deemed in the public domain, this means it is published and generally accessible or available to the public through sales, subscriptions, and libraries. *Id.* A printed book or other printed material setting forth encryption source code is not itself subject to the Export Regulations and thus is outside the scope of the licensing requirement. 15 C.F.R. § 734.3(b)(2) (1998). Notably, however, en-

developing national security concerns.[61] The proliferation and delivery of "unconventional" weapons "pose[d] an urgent threat to security and stability in the Middle East and Persian Gulf region."[62] The AECA authorized the President to regulate the import and export of "defense articles" and "defense services," and to designate such articles and services for inclusion on the USML.[63] Pursuant to 22 U.S.C. § 2778(h), this designation by the President, or a party to whom the President has delegated such authority, is not subject to judicial review.[64] Articles designated by the President as defense articles and defense services are prohibited from international import or export without a license, except as otherwise provided.[65] The President delegated his authority regarding the export of defense articles and services to the Secretary of State pursuant to Executive Order 11,958.[66] In

cryption source code in electronic form or media remains subject to the Regulations. *See id.* § 734.3(b)(3). Scannable materials also remain subject to the licensing requirement where the government deems necessary. 61 Fed. Reg. 68,572, 68,575 (1996); *see, e.g.*, Interview by Dan Charles with Edward Apell, Director, F.B.I. Counter Intelligence, *All Things Considered*, (National Public Radio, Sept. 28, 1995), *cited in* Kerben, *supra* note 56, at 141 n.182.

[61] 22 U.S.C. § 2778 (1994). In the 1980s, nations in the Middle East and Persian Gulf region were responsible for nearly half of the global import and export of weapons and related equipment and services. Foreign Relations Authorization Act, Fiscal Years 1992 and 1993, Pub. L. No. 102-138, § 401(1), 105 Stat. 647, 718 (1991). Nations in this region are the "principal market for the worldwide arms trade." *Id.* The continued reproduction of such weapons, equipment and services facilitate an arms race in these areas where the political, economic, and military environments are precarious. *Id.* § 401(3). "[F]uture security and stability in the Middle East and Persian Gulf region would be enhanced by establishing a stable military balance among regional powers by restraining and reducing both conventional and unconventional weapons." *Id.* § 401(6). "[S]ecurity, stability, peace, and prosperity in the Middle East and Persian Gulf region are important to the welfare of the international economy and to the national security interests of the United States." *Id.* § 401(7). The purpose of § 402, the Multilateral Arms Transfer and Control Regime, includes:

> [T]o slow and limit the proliferation of conventional weapons in the Middle East and Persian gulf region . . .
>
> . . . .
>
> . . . [T]o halt the proliferation of unconventional weapons, including nuclear, biological, and chemical weapons, as well as delivery systems associated with those weapons and the technologies necessary to produce or assemble such weapons . . .
>
> . . . .
>
> . . . [T]o maintain the military balance in the Middle East and Persian Gulf region through reductions of conventional weapons and the elimination of unconventional weapons . . .

Id. § 402(b). Major military equipment referred to in the code is defined as "defense articles and defense services." *Id.* § 402(d)(7). For further discussion of the government's national security concerns, see *infra* Part II.C.

[62] Foreign Relations Authorization Act § 401(4).

[63] 22 U.S.C. § 2778(a)(1) (1994).

[64] *Id.* § 2778(h).

[65] *Id.* § 2778(a)(2).

[66] Exec. Order No. 11,958, 22 C.F.R. § 120.1(a) (1998).

turn, the Secretary of State re-delegated this authority to the Secretary for Arms Control and International Security Affairs.[67]

B. *Jurisdiction Transfer and the Current Government Regulations*

Effective November 15, 1996, pursuant to Executive Order 13,026,[68] control of all nonmilitary encryption items on the USML[69] was transferred from the Department of State to the Department of Commerce,[70] and all nonmilitary encryption items were to be added to the Commerce Control List ("CCL").[71] The explanation of the executive order in the White House Press Release stated: "[T]he export of encryption software, like the export of other encryption products described in this section, must be controlled because of such software's functional capacity, rather than because of any possible informational value of such software."[72]

The Commerce Department regulations ("Export Regulations") control the export of certain software.[73] The Export Regulations prohibit the export of certain encryption software outside the United States unless complex precautions are taken.[74] Posting software on the Internet is considered to be an export under the regulations.[75] The regulations impose additional restrictions which require a license to provide technical assistance to foreign persons with the intent to aid them in the foreign development of items that domestically would be

[67] *Id.*

[68] Exec. Order No. 13,026, 3 C.F.R. 228 (1996-97).

[69] Part 121 of the ITAR sets forth the United States Munitions List. 22 C.F.R. pt. 121. Defense articles are listed in Category XIII(b)(1).

> Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefor, including: (1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software.

22 C.F.R. § 121.1 Category XIII(b)(1) (1996), *amended by* 61 Fed. Reg. 56,895, 68,633 (1997).

[70] Exec. Order No. 13,026, 3 C.F.R. 228.

[71] *See* 15 C.F.R. pt. 774 (Supp. I 1998). Regulatory authority over the export of most encryption products was transferred from the Department of State under the ITAR to the Department of Commerce under the Export Administration Regulations. *Id.*

[72] Exec. Order No. 13,026, 3 C.F.R. 228.

[73] Export is defined as "an actual shipment or transmission of items subject to the [Export Administration Regulations ("EAR")] out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States." 15 C.F.R. § 734.2(b)(1) (1998). Export includes various forms of electronic transfers such as "downloading, or causing the downloading of, . . . software to locations . . . outside the [United States]." *Id.* § 734.2(b)(9)(B)(ii).

[74] *Id.* § 734.2(b)(9).

[75] *Id.* § 734.2(b)(9)(ii)(B).

controlled under other codified regulations.[76] Encryption software is also one item defined as a "defense article" for purposes of regulation under the AECA:

> Software includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair. A person who intends to export software only should, unless it is specifically enumerated in § 121.1 . . . apply for a technical data license pursuant to part 125 of this subchapter.[77]

The Export Regulations provide official procedures required to obtain approval for exporting items on the CCL.[78] To engage in such export, one must first submit a commodity classification request[79] to the Bureau of Export Administration ("BXA").[80] Export Control Classification Numbers are assigned to all items on the CCL and the BXA regulations specify three categories of controlled Encryption Items.[81] Software under Export Classification Numbers 5A002, 5D002 and 5E002 require licenses for export to all foreign destinations except Canada.[82] The regulation provides that after a one-time review by the BXA, licensing exceptions will be available for commercial items such as key recovery software and commodities and non-recovery encryption items up to fifty-six bit key length DES[83] or equivalent strength software.[84] This exception, however, requires that the developer commit to developing recoverable items, also known as

[76] *Id.* § 736.2(b)(7)(ii); *Id.* § 744.9(a). The encryption regulations define technology as the "technical data or technical assistance necessary for the development or use of a product." 22 C.F.R. § 121.1(b)(1) (1996), *amended by* 61 Fed. Reg. 56,895, 68,633 (1997).

[77] 22 C.F.R § 121.8(f) (1998).

[78] 15 C.F.R. pts. 740-44 (1998).

[79] 22 C.F.R. § 120.4 (1998). This procedural requirement is referred to as a commodity jurisdiction request. *Id.* An item for export must be submitted to the Department of State for a determination whether the item is covered by the USML according to the ITAR or the Department of Commerce under the EAR. *Id.* § 120.4(a). This procedure is not intended to determine whether the item may or may not be exported. Rather, it is merely to determine whether the particular commodity is covered by the USML and therefore, whether its export is controlled pursuant to the AECA and the ITAR. *Id.*

[80] 15 C.F.R. pts. 740-44.

[81] Export Classification Number 5A002 encompasses encryption commodities, Classification Number 5D002 covers encryption software, and Classification Number 5E002 covers encryption technology. *Id.* § 742.15(a).

[82] *Id.* The executive order mandating government control of encryption technology explains that the export of encryption products could harm "national security, foreign policy, and law enforcement interests." *Id.* § 742.15.

[83] DES stands for Data Encryption Standard. Marc Davis, *Get The Message?*, J. MARSHALL COMMENT, Winter 1997/98, at 39, 39.

[84] 15 C.F.R. § 742.15(b)(3).

key recovery.[85] "By virtue of holding or having access to a 'backdoor' key, the government is willing to let stronger crypto out into the mainstream or in other words, allow the export of strong crypto."[86] "Key recovery is . . . essentially about resolving a fundamental dilemma of encryption—that is, allowing the use of robust algorithms with long keys, while at the same time providing for code breaking under controlled conditions, for instance, by government officials with a court order."[87]

C. Government National Security Concerns

> Secrecy is a form of power. The ability to protect a secret, to preserve one's privacy, is a form of power. The ability to penetrate secrets, to learn them, to use them, is also a form of power. Secrecy empowers, secrecy protects, secrecy hurts. The ability to learn a person's secrets without her knowledge—to pierce a person's privacy in secret—is a greater power still.[88]

Undeniably, secured communications are essential in today's age of technology. Encryption technology is an invaluable tool necessary for security in electronic communications. As the appreciation for the technology increases, the industry for public encryption devices emerges. It is the growth of this industry that concerns the United States government. The federal government perceives this industry as a threat to national security interests.

The National Security Agency ("NSA") maintains the security of federal communications and data and ensures that the government is

[85] *Id.*· § 742.15(b)(2). Encryption products scramble messages using mathematical sequences. *See* SCHNEIER, *supra* note 2, at 2. A corresponding key is needed to unscramble, or decrypt, the message. *Id.* Recoverable items, such as key escrow or key recovery, means that when data is encrypted a third party retains a copy of the key required to unscramble the information. Smith, *supra* note 2, at 2. The key is retained in an "escrow" by the third party assigned. *See* Dorothy E. Denning, *The U.S. Key Escrow Encryption Technology*, COMPUTER COMM., July 1994, *reprinted in* BUILDING IN BIG BROTHER 111 (Lance J. Hoffman ed., 1995) (demonstrating the basic methodology of key escrow). Such a recovery system facilitates parties when a key is lost, stolen, or tampered with in any way. Smith, *supra* note 2, at 2; *see* NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 284-85 (Kenneth W. Dam & Herb S. Lin eds., 1996). "Escrow became a compromise between the needs of the U.S. national security establishment and the concerns of individuals and businesses." *Encryption Export: Hearings Before the Subcomm. on Int'l Econ. Policy and Trade*, 105th Cong. (1997) (testimony of William A. Reinsch, Under Secretary for Export Administration). Opponents continue to debate over what the government's role in the determination of who the third party key holders (key recovery agents) should be, and to what extent law enforcement agencies could obtain the key if unlawful activity is suspected. *Id.*

[86] Stender, *supra* note 2, at 298 (citing *Encryption Export: Hearings Before the Subcomm. on Int'l Econ. Policy and Trade*, *supra* note 85).

[87] Stender, *supra* note 2, at 307.

[88] Froomkin, *supra* note 5, at 712 (footnotes omitted).

able to intercept and decipher foreign states' codes.[89] The NSA has provided the United States over fifty years of cryptographic services.[90] During World War II, a former United States Army intelligence NSA member decrypted a Japanese code, providing the United States with a rewarding strategic advantage and resulting in Coral Sea and Midway victories.[91] Another NSA predecessor decrypted Japanese messages, albeit not soon enough, forewarning of the bombing of Pearl Harbor.[92] In the early 1960s, the NSA warned the United States of Soviet missions to install offensive missiles in Cuba.[93] The NSA has also played a primary role in designing encryption export control policy. "[T]he State Department relies almost entirely on the NSA to determine what products are subject to a licensing requirement and the licensing policy for such items."[94] The NSA is concerned that the development of the public cryptography industry will threaten its security missions. Continuous growth in private cryptology research could greatly undermine the NSA's control of the science.[95] Private development and reverse engineering, or dissemination, of cryptographic algorithms could alert foreign communicators of flaws in the United States foreign coding system, thereby encouraging foreign parties to modify their codes.[96] These modifications would prevent the NSA from monitoring and deciphering foreign messages—messages potentially carrying terrorist strategies.[97] Finally, the NSA is concerned that the availability of public cryptography abroad would exploit weaknesses in federal code systems or facilitate foreign nations'

[89] *The Government's Classification of Private Ideas: Hearings Before a Subcomm. of the House Comm. on Government Operations*, 96th Cong. 423-26 (1980) (testimony of Adm. B. R. Inman, Director, National Security Agency). More specifically, NSA is responsible for protecting U.S. government information through code creation, intercepting and deciphering foreign communications, and monitoring global messages in and out of the United States. *See Espionage Laws and Leaks: Hearings Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence*, 96th Cong. 25 (1979) (testimony of Daniel B. Silver, General Counsel, National Security Agency).

[90] For a detailed discussion of the NSA and its operations, see generally JAMES BAMFORD, THE PUZZLE PALACE (1982).

[91] *Id.* at 43.

[92] *Id.* at 35-39. Unfortunately the military commanders received the messages without sufficient time to prevent the catastrophic occurrence. *Id.* at 39.

[93] *Id.* at 215.

[94] James B. Altman & William McGlone, *Demystifying U.S. Encryption Export Controls*, 46 AM. U. L. REV. 493, 499 (1996) (footnote omitted).

[95] Admiral B. R. Inman, The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector, Address to the Armed Services Communications and Electronics Association (Mar. 1979), *cited in* Kenneth J. Pierce, *Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation*, 17 CORNELL INT'L L.J. 197, 202 (1984).

[96] *Id.* at 202-03.

[97] *See supra* text accompanying notes 91-93.

rapid advancement of decrypting federal codes.[98] Intercepting and exploiting foreign secrets communicated through electronic signals is essential to United States security.

> To fulfill its mission, of course, the NSA needs to be able to decrypt or "crack" encoded messages. Because there are no restrictions on the sale and use of encryption domestically, controls on exports represent the only effective way for the NSA to limit the level of encryption technology that is deployed overseas.[99]

The Director of the Federal Bureau of Investigation ("FBI") recently stated that "the potential use of such robust encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information poses an extremely serious and in my view unacceptable threat to public safety."[100] Another commentator warned that uncontrolled cryptography is not only subject to abuse by foreign masterminds. "If [unbreakable encryption becomes routine], even the poorest criminals and terrorists in the world would have automatic extreme privacy for their criminal acts."[101]

Undeniably, there is a societal interest in the public use of encryption technology to ensure the privacy and integrity of communication.[102] Simultaneously, however, the same technology threatens law enforcement agencies' ability to control drug traffickers, organized crime, terrorists, and foreign espionage agents.[103] These conflicting interests, among others, have given rise to the encryption export control debate.

III. First Amendment

A. *Categorizing and Balancing Speech*

The government's encryption technology export controls have been challenged as a violation of the First Amendment freedom of speech.

[98] Address by Adm. B. R. Inman, *supra* note 95, at 200.

[99] Altman & McGlone, *supra* note 94, at 499.

[100] The Promotion of Commerce Online in the Digital Era Act of 1996, or Pro-CODE Act, 94th Cong. (1996).

[101] Stender, *supra* note 2, at 324 (citing Steven Levy, *The Cypherpunks vs. Uncle Sam*, N.Y. Times Mag., June 12, 1994, § 6, *reprinted in* Building in Big Brother, *supra* note 85, at 266, 268).

[102] *See* Lance J. Hoffman, *Afterword* to Building in Big Brother, *supra* note 85, at 549.

[103] *Id.* Interestingly, the ability of strong encryption to threaten security officials' access to intelligence information is not greatly debated. Froomkin, *supra* note 5, at 712. The issue debated is to what extent should the government recognize the threat at the expense of, for example, the software industry, see Charles L. Evans, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. Int'l L. & Com. Reg. 469, 488 (1994), or the rights guaranteed by the First Amendment.

The First Amendment to the Constitution of the United States declares that: "Congress shall make no law . . . abridging the freedom of speech."[104] This right of free speech, however, is not absolute.[105] In the view of the Supreme Court, "not all speech is of equal First Amendment importance."[106] Through the interpretation of the First Amendment, the Court established guidelines in determining what speech is protected.[107]

As discussed in Part III.A.1, the Supreme Court employs the categorization method as one means of establishing the First Amendment protection afforded various expressions.[108] This method assigns a category to certain types of speech according to high, middle, or low val-

[104] U.S. CONST. amend. I.

[105] JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW 943 (4th ed. 1991). See Justice Harlan's majority opinion in *Konigsberg v. State Bar of California*, 366 U.S. 36 (1961):

> [W]e reject the view that freedom of speech and association, as protected by the First and Fourteenth Amendments, are "absolutes," not only in the undoubted sense that where the constitutional protection exists it must prevail, but also in the sense that the scope of that protection must be gathered solely from a literal reading of the First Amendment. Throughout its history this Court has consistently recognized at least two ways in which constitutionally protected freedom of speech is narrower than an unlimited license to talk. On the one hand, certain forms of speech, or speech in certain contexts, has been considered outside the scope of constitutional protection. On the other hand, general regulatory statutes, not intended to control the content of speech but incidentally limiting its unfettered exercise, have not been regarded as the type of law the First or Fourteenth Amendment forbade Congress or the States to pass, when they have been found justified by subordinating valid governmental interests, a prerequisite to constitutionality which has necessarily involved a weighing of the governmental interest involved.

Id. at 49-51 (citations omitted). But see Justices Black's absolutist approach to free speech in his dissenting opinion in *Konigsberg*:

> The recognition that [a State] has subjected "speech and association to the deterrence of subsequent disclosure" is, under the First Amendment, sufficient in itself to render the action of the State unconstitutional unless one subscribes to the doctrine that permits constitutionally protected rights to be "balanced' away whenever a majority of this Court thinks that a State might have interest sufficient to justify abridgment of those freedoms. . . . I do not subscribe to that doctrine for I believe that the First Amendment's unequivocal command that there shall be no abridgment of the rights of free speech and assembly shows that the men who drafted our Bill of Rights did all the "balancing" that was to be done in this field.
>
> . . . .
>
> It therefore seems to me that the Court's "absolute" statement that there are no "absolutes" under the First Amendment must be an exaggeration of its own views.

Id. at 60-61, 68 (Black, J., dissenting) (footnotes omitted).

[106] Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758 (1985) (concluding that matter of public concern is of greater constitutional value than matter of purely private concern).

[107] Jeffrey M. Shaman, *The Theory of Low-Value Speech*, 48 SMU L. REV. 297, 298 (1995).

[108] GERALD GUNTHER, CONSTITUTIONAL LAW 1071 (12th ed. 1991). *See generally* Shaman, *supra* note 107, at 341 (demonstrating the application of the categorization approach).

ues.[109] These values receive a varied degree of judicial scrutiny. High valued speech is afforded strict scrutiny,[110] middle valued speech is assigned intermediate scrutiny,[111] and low-value speech is deserving of minimal scrutiny.[112]

The value placed on speech is also determinative of the Court's balancing approach, as discussed in Part III.A.2. The Court applies the ad hoc balancing test to high-value speech,[113] while definitional balancing applies to middle valued speech.[114] Low-value speech is not worthy of any balancing method.[115]

1. *Categorization*

It is difficult to say exactly what characteristics the Court considers in determining the value of specific speech,[116] however, some types are clear. *New York Times v. Sullivan*,[117] perhaps the most celebrated First Amendment case ever decided by the Supreme Court,[118] introduced the proposition that political ideas expressed in written form, even if false,[119] are protected by the First Amendment.[120] Justice

[109] *See* Shaman, *supra* note 107, at 341.

> [T]hrough the technique of categorization . . . the Supreme Court designates different kinds or categories of speech and assigns them high or low value. It can be said that the Court "categorizes" some kinds of speech as beyond First Amendment protection or at the fringes of the First Amendment and therefore entitled to little of its protection.

Id.; *see id.* at 319 (proposing that the Supreme Court has placed some forms of speech in a middle level of the "constitutional hierarchy").

[110] *See* Stromberg v. California, 283 U.S. 359, 369 (1931) ("The maintenance of the opportunity for free political discussion to the end that government may be responsive to the will of the people and that changes may be obtained by lawful means, an opportunity essential to the security of the Republic, is a fundamental principle of our constitutional system.").

[111] *See infra* text accompanying notes 122-24, 143-45.

[112] R.A.V. v. St. Paul, 500 U.S. 377, 400 (1992) (White, J., concurring).

[113] Pierre J. Schlag, *An Attack on Categorical Approaches to Freedom of Speech*, 30 UCLA L. REV. 671, 673 (1983).

[114] MELVILLE B. NIMMER, NIMMER ON FREEDOM OF SPEECH §§ 2-15 to 2-24 (1984).

[115] Shaman, *supra* note 107, at 331.

[116] *See id.* at 298-301.

[117] 376 U.S. 254 (1964).

[118] *See* ANTHONY LEWIS, MAKE NO LAW: THE SULLIVAN CASE AND THE FIRST AMENDMENT (1991); Harry Kalven, Jr., *The* N.Y. Times *Case*: *A Note on "The Central Meaning of the First Amendment*," 1964 SUP. CT. REV. 191.

[119] *Sullivan*, 376 U.S. at 279 n.19 ("Even a false statement may be deemed to make a valuable contribution to public debate."). The Court proposed that inevitable erroneous statements must be protected to ensure the survival of free speech. *Id.* at 271-72. In order to promote valid criticism of public officials, the First Amendment needs "breathing space," thereby allowing a defense in a suit for libel for "erroneous statements honestly made." *Id.*

[120] In *Sullivan*, a Commissioner of the City of Montgomery, Alabama, claimed he was libeled by an advertisement in the *New York Times* newspaper. *Id.* at 256. The advertisement described in detail alleged forceful, egregious police actions. *Id.* The court conceded that some of the statements were not entirely accurate, but found that an "erroneous statement is inevita-

Brennan's majority opinion reminded us that "debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."[121]

Middle-value speech is valued somewhat greater than low-value speech, but significantly lower than high-value speech.[122] Identifying an example of middle-value speech is not as clear as high-value political speech. The Supreme Court placed commercial speech, for example, "at the bottom of a middle level of the constitutional hierarchy."[123] The Supreme Court reasoned that commercial speech does "no more than propose a commercial transaction."[124]

The Court has identified three factors which strongly identify commercial speech when existing in combination: (1) advertisement; (2) mentioning a specific product by name; and (3) the speech is economically motivated.[125] In *Bolger v. Youngs Drug Products Corp.*,[126] the combination of *all* these characteristics provided strong support for the conclusion that informational pamphlets regarding contraceptives were commercial speech.[127]

The Supreme Court has noted that consumers and society as a whole have a great concern for the free flow of commercial information.[128] In *Virginia State Board of Pharmacy v. Virginia Citizens Con-*

ble in free debate." *Id.* at 271. Establishing libel of a public official under *Sullivan*, the plaintiff is required to prove: first, the defamatory statement related to the government official claiming libel, *id.* at 288; second, the statement must be false, *id.* at 271; and third, and most importantly, the plaintiff must provide proof that the defendant made the defamatory statements with "actual malice," i.e., knowledge that the statement was false or reckless disregard of the statement's falsity. *Id.* at 281.

[121] *Id.* at 270; *see* Terminiello v. Chicago, 337 U.S. 1, 4 (1949); DeJonge v. Oregon, 299 U.S. 353, 365 (1937).

[122] *See infra* notes 143-48 and accompanying text.

[123] Shaman, *supra* note 107, at 319 ("While more valuable forms of speech are entitled to the protection of strict judicial scrutiny, commercial speech receives the protection of intermediate scrutiny, a step up, of course, from minimal scrutiny, but a significant step down from strict scrutiny."). Justice Stevens, however, argued some forms of "promotional advertising" should not be categorized with other commercial speech because the expression may in fact relate to issues of public significance. Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 579-81 (1980) (Stevens, J., concurring) (holding statute banning electrical utility promotional advertising violates First Amendment). Therefore, argued Stevens, promotional advertising should be entitled to high-value protection. *Id.*

[124] Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations, 413 U.S. 376, 385 (1973) (holding proposals of possible employment, such as the advertisement at issue, are not protected by the First Amendment).

[125] Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 66-67 (1983) (finding contraceptive ad mailings constitute commercial speech).

[126] *Id.*

[127] *Id.*

[128] *See supra* notes 122-24 and accompanying text.

sumer Council, Inc.,[129] the Court stated that advertising propagates information that is fundamental to intelligent decision-making about purchasing goods and services.[130]

Categories of speech qualifying as low-value are similarly difficult to clearly identify.[131] As previously mentioned, the Court theorizes that some categories of speech have less value than others. This theory, "marked by vacillation and uncertainty,"[132] creates difficulties in determining exactly what categories of speech the Court classifies as low in value. Obscenity has been upheld as low-value speech.[133] Child pornography has also been labeled as low-value.[134] In *R.A.V. v. St. Paul*,[135] Justice White's concurring opinion characterized low-value speech as expressing content "worthless or of *de minimis* value to society."[136]

Categorizing speech as high, middle, or low-value is legally relevant in that it determines the level of scrutiny applied to the regulation suppressing such speech.[137] High-value speech is subject to strict scrutiny under the First Amendment.[138] At this level, the regulating body must establish a compelling state interest that must be achieved by the least intrusive means.[139] As mentioned earlier, political speech is con-

[129] 425 U.S. 748 (1976).

[130] *Id.* at 765.

[131] Shaman, *supra* note 107, at 299.

> At one time or another, the Court has ruled that fighting words, obscenity, and child pornography are of low value. Some members of the Court, though not quite a majority, would add non-obscene sexually explicit expression to that list. On occasion, a few members of the Court have expressed doubt about the value of profanity, but profane speech still clings to a valued position in the minds of a majority of the Court. In the area of libel, the Court has said that "there is no constitutional value in false statements of fact," and that libelous speech on purely private matters is of less First Amendment concern.

Id. (quoting Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974)).

[132] *Id.*

[133] *See* Paris Adult Theatre I v. Slaton, 413 U.S. 49, 58 (1973) (denying protection of obscene materials based on a connection between obscenity and crime and other antisocial conduct); Miller v. California, 413 U.S. 15, 24-25 (1973) (proposing a new definition of obscenity as "lack[ing] serious literary, artistic, political, or scientific value."); Roth v. United States, 354 U.S. 476, 485-92 (1957) (holding that prohibiting the distribution of obscene materials did not violate the First Amendment).

[134] New York v. Ferber, 458 U.S. 747, 762 (1981) ("[T]he value of permitting live performances and photographic reproductions of children engaged in lewd sexual conduct is exceedingly modest, if not *de minimis.*").

[135] 505 U.S. 377 (1992).

[136] *Id.* at 400 (joined by Blackmun and O'Connor, JJ.).

[137] *See* Jeffrey M. Shaman, *Constitutional Fact: The Perception of Reality By the Supreme Court*, 35 U. FLA. L. REV. 236, 242-52 (1983).

[138] *Id.* at 245.

[139] *Id.*

sidered to be at the core of protected speech.[140] Criticism of government remains "at the very center of the constitutionally protected area of free expression."[141] In order for the state to justify prohibiting such expression of an opinion, "it must be able to show that its action was caused by something more than a mere desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint."[142]

The Court meanwhile applies intermediate scrutiny to middle-value speech, which does not deserve the highest level of protection yet has some societal value.[143] Intermediate scrutiny requires the regulation to be justified by an important governmental interest achieved through narrowly-tailored means.[144] The means, however, need not be perfect.[145] As mentioned earlier, commercial speech[146] is one example of middle-value speech deserving only intermediate scrutiny.[147] The Constitution protects commercial speech to a lesser degree than strict scrutiny, but more than minimal.[148]

Low-value speech is afforded only minimal scrutiny.[149] Minimal scrutiny requires that the regulating body establish a "valid or legiti-

[140] New York Times v. Sullivan, 376 U.S. 254, 292 (1964); *see supra* notes 112-17.

[141] *Sullivan*, 376 U.S. at 292. See *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969), where students wore black armbands to oppose the Vietnam War. *Id.* at 514. Not only was this form of speech "closely akin to 'pure speech,'" *id.* at 505, but it was in opposition to the government's involvement in the Vietnam War. *Id.* at 510. Thus, the regulation was subject to strict scrutiny. *Id.* at 513. The Court did not expressly use the term "compelling" to explain the burden of proof, but required the government to establish that the conduct "materially and substantially interfere[d] with the requirements of appropriate discipline in the operation of the school." *Id.* The State in this case could not meet its burden of proof where the record was void of evidence establishing anticipated substantial disruption or of material interference with academic activities and where no disruptions or interferences in fact occurred. *Id.* at 514.

[142] *Tinker*, 393 U.S. at 509.

[143] Shaman, *supra* note 107, at 329.

[144] *Id.*

[145] *Id.* (citing Shaman, *supra* note 137, at 242-52).

[146] Commercial speech is defined as proposing a commercial transaction. NOWAK & ROTUNDA, *supra* note 105, at 1011. Commercial speech was not always afforded protection. "Until relatively recently the Court has simply excluded all commercial speech, even truthful advertising, from the coverage of the First Amendment." *Id.* Today, commercial speech is vested with First Amendment protection, but not as extensive as political speech. "The state can issue reasonable time, place, or manner regulations of commercial speech. . . . In addition, the state has a broader power to regulate misleading commercial speech than its power to regulate misleading or libelous speech about public officials or public figures." *Id.*

[147] *See* Shaman, *supra* note 107, at 329; *see also* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 562 (1980) (determining commercial speech is expression protected by the First Amendment but noting there is a "commonsense" difference between traditionally protected speech and commercial speech).

[148] Shaman, *supra* note 107, at 319, 329; *see Central Hudson*, 447 U.S. at 562.

[149] Shaman, *supra* note 107, at 330.

mate state interest achieved through reasonable means."[150] This level of scrutiny grants tremendous deference to the state in its decision-making power and thus is effectively no scrutiny at all.[151] Occasionally, however, the Court will strike down a "low-value speech" regulation by applying minimal scrutiny with "bite."[152]

A common criticism of the categorization method is the tendency of speech to cross categories.[153] "[T]he categories of speech designated by the Supreme Court, like most other categories, cannot be neatly separated. They tend to overlap one another, making it problematic to assess the value of speech."[154] For example, an obscene statement is afforded minimal protection,[155] but an obscene comment critical of the government presumably would deserve intermediate, if not strict, scrutiny. On the other hand, an obscene comment critical of the government causing physical harm to another person or group of persons would likely be struck down because of the harm it caused.[156] Notably, however, "a certain amount of categorizing is unavoidable in constitutional decision-making, or, for that matter, in any other form of human decision-making."[157]

[150] *Id.*

[151] *Id.*

[152] *Id.*; *see* Jeffrey M. Shaman, *Cracks in the Structure: The Coming Breakdown of the Levels of Scrutiny*, 45 OHIO ST. L.J. 161, 166-68 (1984).

[153] *See* Shaman, *supra* note 107, at 344-45 (proposing categories of speech tend to overlap and thus confuse the value attributed to such expression).

[154] *Id.* at 345; *see* Cohen v. California, 403 U.S. 15 (1971) (concluding publicly displaying a jacket with words "Fuck the Draft" is speech protected by the First Amendment, thereby apparently categorizing "Fuck the Draft" as both political speech and profanity); *see also* Hustler Magazine v. Falwell, 485 U.S. 46, 50-52 (1988) (demonstrating difficulty in categorizing an undeniably gross and offensive parody that also skewers political and religious hypocrisy).

[155] Shaman, *supra* note 107, at 308 ("Obscene speech . . . remains at the bottom of the totem pole, having, as the Court sees it, no value and therefore no protection under the First Amendment."); *see* Roth v. United States, 354 U.S. 476, 484 (1957) (demonstrating obscene speech is worthy of minimal First Amendment protection).

[156] *See* Paris Adult Theatre I v. Slaton, 413 U.S. 49, 58 (1973) (holding the distribution of obscene materials to be prohibited because obscenities were somehow connected to crime and other anti-social behavior). In 1978, the Supreme Court demonstrated an example of such classification cross-over. *Compare* Ohralik v. Ohio State Bar Ass'n, 436 U.S 447, 459 (1978) (upholding a lawyer solicitation regulation in a commercial environment) *with In re* Primus, 436 U.S. 412, 433-39 (1978) (striking down a lawyer solicitation regulation in a political environment).

[157] Shaman, *supra* note 107, at 342; *see* Geoffrey R. Stone, *Content Regulation and the First Amendment*, 25 WM. & MARY L. REV. 189 (1983).

> [T]he low value theory, or some variant thereof, is an essential concomitant of an effective system of free expression, for unless we are prepared to apply the same standards to private blackmail, for example, that we apply to public political debate, some distinctions in terms of constitutional value are inevitable.

Id. at 252 n.24; *see* Cass R. Sunstein, *Pornography and the First Amendment*, 1986 DUKE L.J. 589, 605 ("[I]t would be difficult to imagine a sensible system of free expression that did not distin-

2. *Balancing*

In addition to levels of scrutiny, the Court applies various balancing approaches to categories of speech. High-value speech is subject to an ad hoc balancing approach where the Court focuses upon each particular case individually and weighs the interest served by the speech in each particular instance against the asserted state interest in regulating the speech.[158] As mentioned earlier, no speech is absolutely protected.[159] The ad hoc balancing test, however, tends to be highly protective of high-value speech.[160] "[The ad hoc balancing test] allow[s] speech to be regulated only upon a showing that the particular speech in question will cause a serious harm that cannot be avoided by an alternative, less restrictive regulation."[161] Notably, if the government has a compelling state interest in preventing serious harm caused by highly valued speech, a regulation of such speech may be constitutional.[162] Therefore, even political speech, the most valued kind of speech, may be regulated if it is demonstrated to cause serious harm, or if a compelling state interest is shown to support its regulation.[163]

Ad hoc balancing applies to high-value speech. Lower valued speech, though not the least valued speech, is subject to definitional balancing.[164] The definitional balancing approach does not require the Court to find that the speech in a particular case is harmful.[165] The Court must simply determine that the category of speech "tends to cause harm."[166] Therefore, when applying definitional balancing, the Court will uphold a regulation of speech if the Court is convinced

guish among categories of speech in accordance with their importance to the underlying purposes of the free speech guarantee.").

[158] Schlag, *supra* note 113, at 673.

[159] *See supra* note 105 and accompanying text.

[160] See *Brandenburg v. Ohio*, 395 U.S. 444 (1969), where a leader of a Ku Klux Klan ("KKK") group challenged his conviction under an Ohio statute which punished advocates of violent means when attempting to achieve political and economic change. *Id.* at 444-45. The appellant discussed the KKK's plan to march on Congress during a televised broadcast of his presentation at the rally. *Id.* at 445. The Court held advocacy of violence protected by the First Amendment as long as the advocacy did not incite people to imminent action. *Id.* at 447. "[The state may not] forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *Id.* (footnote omitted).

[161] Shaman, *supra* note 107, at 330-31.

[162] *Id.* at 331.

[163] *Id.*

[164] NIMMER, *supra* note 114, §§ 2-15 to 2-24.

[165] Shaman, *supra* note 107, at 331.

[166] *Id.*

that the class of speech in question is sufficiently harmful, even without a showing of actual harm.[167]

Speech that the Court finds lowest in value, such as obscenity, is denied definitional balancing.[168] Professor Jeffrey Shaman described the Supreme Court's approach to speech lowest in value:

> [B]ecause the Court sees the speech as having little or no value, the Court designates it as a category of speech that receives no First Amendment protection. In effect, the Court "categorizes out" certain kinds of speech to deny them First Amendment protection. This use of the categorization technique requires no showing of any harm, whether of the particular speech or of the class of speech. All the Court looks to is the value of the speech, and if the Court is convinced that the speech has no value, the Court gives no constitutional protection to the speech.[169]

Summarizing these tests, courts apply the balancing approach to determine the constitutionality of a regulation based on an evaluation of the harm caused by the speech. Courts apply the categorization approach to determine an expression's constitutionality through value assessment.

B. *Pure Speech Versus Expressive Conduct*

The Supreme Court applies the classification and balancing techniques in resolving a First Amendment protection issue. Additionally, the Court assesses labels to various forms of speech. The purest forms of speech are the printed page and the spoken word.[170] However, even speech not in the precise form of written or verbal words, or expressive conduct, is granted First Amendment protection as it is "closely akin to 'pure speech.'"[171] For example, in *Tinker v. Des Moines Independent Community School District*,[172] the Court protected the wearing of black armbands by school children in opposition to the Vietnam War.[173]

Additionally, some types of expressive conduct, although not pure speech or "closely akin to pure speech"[174] receive constitutional pro-

[167] *Id.* at 331-32.

[168] *Id.* at 331.

[169] *Id.* at 331-32.

[170] *See* Shaman, *supra* note 107, at 304.

[171] Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503, 513 (1969) ("[W]e do not confine the permissible exercise of First Amendment rights to a telephone booth or the four corners of a pamphlet, or to supervised and ordained discussion in a school classroom.").

[172] *Id.* at 514.

[173] *Id.*

[174] *See supra* text accompanying note 171.

tection.[175] Not all expressive conduct, however, is per se protected speech. The Court in *United States v. O'Brien*[176] explicitly stated: "We cannot accept the view that an apparently limitless variety of conduct can be labeled 'speech' whenever the person engaging in the conduct intends thereby to express an idea."[177]

Another labeling issue arises where speech is not purely expressive, but also contains non-speech elements. If the Court determines a regulation suppresses expressive conduct where both speech and non-speech elements are present, the Court must examine which element the government intended to regulate.[178] The *O'Brien* Court held that "when 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the 'nonspeech' element can justify incidental limitations on First Amendment freedoms."[179] The extent to which the governmental interest must be established depends on the value the Court gives to the speech at issue.[180] After all, "not all speech is of equal First Amendment importance."[181]

C. *Content-Based or Content-Neutral*

After a court categorizes the type of speech and determines the applicable test, it must then focus on the government's conduct. Where the government attempts to regulate conduct, courts first consider whether the regulation discriminates based on the content of protected speech. Viewpoint discrimination and subject-matter discrimi-

[175] In *Stromberg v. California*, 283 U.S. 359 (1931), the Court found that a statute criminalizing the display of a red flag "as a sign, symbol or emblem of opposition to organized government" without proof of likelihood to incite violence, was unconstitutional as a violation of freedom of speech. *Id.* at 369-70. Thus, the Court demonstrated that speech does not need to be in the form of words to be protected by the First Amendment. *See* Texas v. Johnson, 491 U.S. 397, 405 (1989) (holding the burning of the American flag to be expressive conduct). In *Johnson*, a demonstrator burned the American flag to protest the government in a political demonstration. *Id.* at 399. The Court held the burning of the American flag to be expressive conduct. *Id.* at 405. The Court recognized that First Amendment protection applied to "speech" other than the written or spoken word. *Id.* at 404. By no means did the Court intend to find that any conduct is protected speech as long as the actor intends to convey a message. *Id.* at 405. The Court noted the American flag, like many other flags, possesses an inherent message. *Id.* ("The very purpose of a national flag is to serve as a symbol of our country; it is, one might say, 'the one visible manifestation of two hundred years of nationhood.'") (citing Smith v. Goguen, 415 U.S. 566, 603 (1974) (Rehnquist, J., dissenting)).

[176] 391 U.S. 367 (1968).

[177] *Id.* at 376.

[178] *Id.*

[179] *Id.*

[180] *Id.* at 376-77.

[181] Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758 (1985); *see supra* notes 106-07 and accompanying text.

nation are two forms of content-based regulations.[182] If a regulation is based on a particular viewpoint[183] or subject matter,[184] the Court applies strict scrutiny.[185] According to Justice Marshall, "[A]bove all else, the First Amendment means that government has nó power to restrict expression because of its message, its ideas, its subject matter, or its content."[186] Format discrimination, meanwhile, is a content-neutral regulation that warrants a less strict level of scrutiny.[187] Pro-

[182] *See* GUNTHER, *supra* note 108, at 1214-17. We must remember that although content-based regulations are not permitted, it is often necessary to review the content of the speech to determine whether or not the speech is protected by the First Amendment. *See* Young v. American Mini Theatres, 427 U.S. 50, 66 (1976) (noting even protected speech may or may not be regulated depending on the content of the speech); New York Times v. Sullivan, 376 U.S. 254, 279-80 (1964) (recognizing that a public official may recover damages for libel if it can be proven the critic wrote with actual malice). One may reasonably assume that if the content had been referring to a private citizen, thus altering the subject matter, the burden of proof would be lessened. These cases do not belie the general principle prohibiting content-based regulation. The purpose of the principle is to ensure government neutrality in its regulation. *See* Turner Broad. v. FCC, 512 U.S. 622, 642 (1994) ("The principle inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of [agreement or] disagreement with the message it conveys.") (citing Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989)). The regulation may not be influenced by personal sympathy or hostility for the message of the speaker, writer, actor, or any other form of communicator. *Young*, 427 U.S. at 68 ("Thus, although the content of story must be examined to decide whether it involves a public figure or a public issue, the Court's application of the relevant rule may not depend on its favorable or unfavorable appraisal of that figure or that issue.").

[183] For example, a regulation that permits Democrats to speak, but not Republicans, or a regulation that allows presentations by pro-choice activists, but not pro-life activists.

[184] *See, e.g.*, Carey v. Brown, 447 U.S. 455, 460-61 (1980) (striking down state law barring picketing of residences or dwellings, but permitting peaceful picketing of a place of employment involved in a labor dispute); Police Dep't v. Mosley, 408 U.S. 92, 92-94 & n.2 (1972) (finding unconstitutional ordinance which barred picketing within 150 feet of a school, but exempted "peaceful picketing of any school involved in a labor dispute").

[185] GUNTHER, *supra* note 108, at 1214. Professor Geoffrey Stone, one of the leading defenders of the distinction between the levels of scrutiny afforded content-based versus content-neutral regulations, explains the justification for a higher level of scrutiny afforded viewpoint discrimination:

> Any law that substantially prevents the communication of a particular idea, viewpoint, or item of information violates the [F]irst [A]mendment except, perhaps, in the most extraordinary of circumstances. This is so, not because such a law restricts "a lot" of speech, but because by effectively excising a specific message from public debate, it mutilates "the thinking process of the community" and is thus incompatible with the central precepts of the [F]irst [A]mendment.

Stone, *supra* note 157, at 198 (quoting ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM 27 (1960)).

[186] *Mosley*, 408 U.S. at 95 (citations omitted).

[187] GUNTHER, *supra* note 108, at 1214; *see* Members of City Council v. Taxpayers for Vincent, 466 U.S. 789, 804-05 (1984) (holding an ordinance prohibiting posting signs on public property constitutional); Young v. American Mini Theatres, 427 U.S. 50, 61 (1976) (prohibiting all adult films in a particular area). In *Taxpayers for Vincent*, Justice Stevens's majority opinion classified the ordinance as content-neutral. *Taxpayers for Vincent*, 466 U.S. at 804-07.

> The ordinance prohibits appellees from communicating with the public in a certain manner, and presumably diminishes the total quantity of their communication in the

fessor Gerald Gunther opines that although format discriminations do not involve viewpoint or subject matter discrimination, they do afford special treatment to expressions protected by the First Amendment:

> A total ban on a particular format may in fact have a major effect on the quantity of communication. Moreover, it may in fact discriminate against those groups who are financially unable to resort to the more conventional (and more expensive) means of communication, such as newspapers and the broadcasting media.[188]

The Court today, however, typically upholds a majority of format-based regulations.[189] "[C]ontent-based restrictions are very strictly scrutinized; content-neutral distinctions elicit a scrutiny less strict."[190]

D. *The* O'Brien *Test*

In an attempt to constitutionally challenge the government's regulation of exporting encryption technology as a suppression of expressive conduct, courts have applied the *O'Brien* test. In *United States v. O'Brien*,[191] the defendant was convicted for violating a statute that prohibited knowingly destroying or mutilating certificates such as registration certificates for the Selective Service.[192] Reviewing the statute, the Court found that O'Brien's certificate burning was expressive conduct where he intended to express his beliefs and influence the public.[193] He knew burning the certificate was a violation of federal law and others would understand the certificate burning was in opposition to the war.[194] The regulation, however, was content-neutral as it attempted to prohibit knowing destruction of certificates issued by the Selective Service System.[195] O'Brien was convicted for deliberately destroying his registration certificate, thus willfully frustrating

> City. . . . [But it] has been clear since this Court's earliest decisions . . . [that] the state may sometimes curtail speech when necessary to advance a significant and legitimate state interest. . . . [The] First Amendment forbids the government from regulating speech in ways that favor some viewpoints or ideas at the expense of others. . . . That general rule has no application to this case. For there is not even a hint of bias or censorship in the City's enactment or enforcement of this ordinance.

Id. at 803-04. The Court's review required a showing that the statute promoted an important or substantial governmental interest unrelated to the suppression of expression and the "'incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.'" *Id.* at 804-05 (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

[188] GUNTHER, *supra* note 108, at 1217.

[189] *Id.*; *see, e.g.*, *Taxpayers for Vincent*, 466 U.S. at 817.

[190] GUNTHER, *supra* note 108, at 1214.

[191] 391 U.S. 367 (1968).

[192] *Id.* at 370.

[193] *See id.* at 376.

[194] *Id.* at 369-70.

[195] *Id.* at 375.

the governmental interest of "preventing harm to the smooth and efficient functioning of the Selective Service System."[196] The Court explicitly stated: "For this noncommunicative impact of his conduct, and for nothing else, he was convicted."[197]

The Court applied a four-part test to determine the constitutionality of a content-neutral regulation[198] that attempted to suppress conduct[199] with speech and non-speech elements:[200] (1) the government must have the authority to regulate this activity; (2) the regulation must further an important or substantial governmental interest;[201] (3) the purpose must be unrelated to regulating free speech; and (4) the regulation must be "no greater than is essential to the furtherance of that interest."[202] The Court applied this test to the government regulation and upheld the defendant's conviction.[203] First, the Court found the government had the authority to regulate this activity.[204] Second, the Court expressly held that the regulation of burning of certificates such as the draft cards furthered the government's substantial and legitimate interest in keeping track of the draft cards in a time of war.[205] Third, the government's purpose was found to be unrelated to regulating free speech, as the government wanted to ensure that people had their draft cards for tracking purposes.[206] Finally, the Court found that the regulation clearly protected this stated substantial governmental interest.[207] Furthermore, there were no alternative means that would be more narrowly tailored to achieve the government's purpose of protecting the availability of the certificates.[208] Notably, the Court stated that even if there had been an identified communica-

[196] *Id.* at 382.

[197] *O'Brien*, 391 U.S. at 382. *But see* Stromberg v. California, 283 U.S. 359, 369-70 (1931) (finding statute prohibiting the display of any "flag, badge, banner, or device" as a means of expressing opposition to organized government unconstitutional as the statute was aimed at suppressing communication).

[198] *See O'Brien*, 391 U.S. at 376 (proposing that if the governmental interest is really aimed at the speech or expression, the Court must apply strict scrutiny).

[199] *Id.* (describing the process of determining conduct as expressive when the communicator intended to convey a particularized message and presumably the message would be understood by those who viewed it).

[200] *Id.*

[201] *Id.* at 377 (holding that the *O'Brien* test applies intermediate scrutiny to regulation aimed at expressive conduct as long as the intent is not to suppress the speech).

[202] *Id.*

[203] *Id.*

[204] *O'Brien*, 391 U.S. at 377.

[205] *Id.* at 377-81.

[206] *Id.* at 378-82.

[207] *Id.* at 381.

[208] *Id.* The Court concluded that the defendant was convicted for his conduct and not for any communicative impact his conduct may have provided. *Id.* at 382.

tive element in the defendant's conduct, this alone would not place the conduct under protection of the First Amendment: "[W]hen 'speech' and 'non-speech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the non-speech element can justify incidental limitations on First Amendment freedoms."[209]

In *Texas v. Johnson*,[210] the Court applied the *O'Brien* test to a statute criminalizing the intentional or knowing desecration of venerated objects.[211] The Court asserted that burning the American flag was expressive conduct that others could understand as a message that the defendant was intending to convey.[212] Unlike *O'Brien*, the Court found that the government was attempting to regulate the speech as opposed to the conduct.[213] A regulation attempting to protect the positive message conveyed by the flag is content-based and therefore subject to strict scrutiny.[214] "If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[215] Hence, the restriction of a message based on its content takes a regulation out of the realm of the *O'Brien* test and strict scrutiny applies.[216]

[209] *Id.*

[210] 491 U.S. 397 (1989).

[211] *Id.* at 400. The defendant, Gregory Lee Johnson, participated in a demonstration protesting the Reagan Administration's policies on nuclear weapons. *Id.* at 399. In front of Dallas City Hall, Johnson bathed the American Flag in kerosene and ignited the flag, submerging it in a bed of flames. *Id.* As the flag burned, fellow protesters chanted anti-America poetry. *Id.* Several witnesses testified that Johnson's flag burning demonstration was personally offensive. *Id.* No one was physically injured or threatened with such injury. *Id.* Johnson was charged with desecrating a venerated object in violation of the Texas statute. *Id.* at 400. He was convicted for desecrating the flag and not for the insulting words he chanted. *Id.* at 402.

[212] *Id.* at 411.

> If [the defendant] had burned the flag as a means of disposing of it because it was dirty or torn, he would not have been convicted of flag desecration under this Texas law: federal law designates burning as the preferred means of disposing of a flag "when it is in such condition that it is no longer a fitting emblem for display."

Id. (citations omitted).

[213] *Id.* at 412.

[214] *Id.* ("[The defendant] was not . . . prosecuted for the expression of just any idea; he was prosecuted for his expression of dissatisfaction with the policies of this country, expression situated at the core of our First Amendment values.") (footnote omitted).

[215] *Id.* at 414.

[216] *Johnson*, 491 U.S. at 412. The Court cited *Boos v. Barry*, 485 U.S. 312, 321 (1988), for the proposition that the State's interest in preserving the "special symbolic character of the flag" subjects the Texas statute to strict scrutiny. *Johnson*, 491 U.S. at 412.

E. Prior Restraints and the First Amendment

As previously mentioned, the Court applies a variety of tests to determine if and how much constitutional protection is afforded an alleged expression. The Supreme Court applies additional tests to regulations functioning as a prior restraint on speech. "[I]t has been generally, if not universally, considered that it is the chief purpose of the [First Amendment's free press] guaranty to prevent previous restraints upon publication."[217] The proprietary status afforded publication justifies the Court's presumption of unconstitutionality when faced with a prior restraint. "Any prior restraint on expression comes to [the] Court with a 'heavy presumption' against its constitutional validity."[218] While prior restraints have often applied to publications,[219] they are also recognized in licensing schemes.[220] Notably, however, the Court has consistently rejected the idea that a prior restraint can never be employed.[221]

The government's encryption export regulation has been challenged as an unconstitutional licensing scheme. When licensing schemes function as a prior restraint on speech, *Freedman v. Maryland*[222] and *City of Lakewood v. Plain Dealer Publishing Co.*[223] provide reviewing guidelines.

In *Freedman*, the state enacted a statute requiring submission of all motion pictures to the censorship board prior to exhibition.[224] The appellant was convicted for failing to submit a movie to the board prior to its showing.[225] He argued that the licensing scheme was an unconstitutional prior restraint, since the statute did not provide a time limit for judicial review and the statutory procedure effectively barred exhibition without a time consuming appeal for reversal of the review board's decision.[226] The Court found that the state procedural

[217] Near v. Minnesota, 283 U.S 697, 713 (1931). In *Near*, a Minnesota statute forbade producing and publishing "malicious, scandalous and defamatory" periodicals. *Id.* at 701-02. Such an injunction was found unconstitutional as a prior restraint on speech. *Id.* at 723. "*Near v. Minnesota* . . . is the most frequently cited case symbolizing the special suspicion of prior restraint." GUNTHER, *supra* note 108, at 1203 n.3.

[218] Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971) (citations omitted).

[219] *See e.g.*, CBS v. Davis, 510 U.S. 1315 (1994); New York Times Co. v. United States, 403 U.S. 713 (1971).

[220] *See, e.g.*, FW/PBS, Inc., v. City of Dallas, 493 U.S. 215 (1990); City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 755-56 (1988).

[221] Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 570 (1976).

[222] 380 U.S. 51 (1965).

[223] 486 U.S. 750 (1988).

[224] *Freedman*, 380 U.S. at 52.

[225] *Id.* at 53.

[226] *Id.* at 54-55.

scheme constituted an invalid prior restraint.[227] Some cases applying the *Freedman* standards interpret the Court's opinion to hold that for a licensing scheme to be constitutional: (1) the licensor must make the licensing decision within a specific and reasonable period of time; (2) there must be prompt judicial review; and (3) the censor bears the burdens of going to court to uphold a licensing denial and justifying the denial.[228]

In *Lakewood*, the Court did not apply the *Freedman* factors. Instead, the Court found that in order to strike down a licensing scheme by a prior restraint facial challenge, the scheme must give "a government official or agency substantial power to discriminate based on the content or viewpoint of speech by suppressing disfavored speech or disliked speakers."[229] In order to facially attack a licensing scheme, the licensing law "must have a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of the identified censorship risks."[230] The mere fact that regulated conduct possibly can be expressive is not enough to invalidate a law on its face on prior restraint grounds.[231] Furthermore, a licensing scheme must be directed "narrowly and specifically at expression or conduct commonly associated with expression."[232]

[227] *Id.* at 58-60. In its opinion, the Court identified several constitutionally mandated safeguards:

> First, the burden of proving that the film is unprotected expression must rest on the censor. . . . [Second, the licensing scheme] cannot be administered in a manner which would lend an effect of finality to the censor's determination whether a film constitutes protected expression. . . . [Because] only a judicial determination in a adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a 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 judicial determination on the merits must similarly be limited to preservation of the status quo for the shortest fixed period compatible with sound judicial resolution.

Id. at 58 (citations omitted).

[228] *See* FW/PBS, Inc. v. Dallas, 493 U.S. 215, 227 (1990).

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

[230] *Id.*

[231] *See* Roulette v. City of Seattle, 97 F.3d 300, 303 (9th Cir. 1996) (proposing that laws prohibiting sitting on city sidewalks are not subject to facial challenge even though sitting on city sidewalks may occasionally be expressive).

[232] *Lakewood*, 486 U.S. at 760-61 (reasoning that "laws of general application that are not aimed at conduct commonly associated with . . . expression carry with them little danger of censorship").

IV. Constitutional Challenges to Encryption Export Regulations[233]

A. Karn v. United States Department of State

In 1994, Karn brought the first case challenging the constitutional validity of government encryption regulations.[234] He submitted a commodity jurisdiction request[235] to the State Department for the book *Applied Cryptography*, by Bruce Schneier.[236] The Office of Defense Trade Controls ("ODTC") determined that the book itself was not subject to the jurisdiction of the Department of State under the ITAR.[237] The two diskettes referred to in the book, however, contained encryption source code and therefore were potentially subject to the licensing jurisdiction of the Department of State.[238] Therefore, on March 9, 1994, Karn submitted a commodity jurisdiction request for a diskette containing the encryption source code referred to in the government's response to Karn's first submission.[239] The ODTC found the diskette subject to the jurisdiction of the Department of State pursuant to the ITAR and the AECA as a defense article on the United States Munitions List.[240] Karn's appeal was denied and the source code diskette was confirmed as a defense article on the Munitions List.[241] In response, Karn filed a complaint with the District Court of the District of Columbia.[242]

The district court granted the government's summary judgment motion, holding that the government properly designated cryptographic

[233] The Export Regulations have come under Congressional attack as well as constitutional challenges. For example, a number of bills have come before Congress proposing the relaxation of export controls on encryption exportation. *See Showdown on Encryption*, WASH. POST, May 25, 1997, at C6. "While congressional efforts appear to be motivated mostly by financial or international trade concerns, court challenges find their predicate on constitutional grounds." Stender, *supra* note 2, at 308-09. For an outline of the pending proposals before Congress, see *id.* at 309. This Comment focuses on the constitutional challenges to encryption licensing controls.

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

[235] See *supra* note 79 for a description of the commodity jurisdiction request process.

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

[237] *Id.*

[238] *Id.*

[239] *Id.* at 3-4.

[240] *Id.* at 4.

[241] *Id.*

[242] *Karn*, 925 F. Supp. at 4.

software on the list of defense articles.[243] The court denied judicial review of the issue.[244]

The district court then addressed the government's request for judgment as a matter of law on Karn's First Amendment claim.[245] Karn contended that the diskette[246] was "speech" protected by the First Amendment, because the source code contained human readable "comments" which are ignored by the computer.[247] The court accepted this claim.[248]

The court found the government regulation content-neutral.[249] The governmental interest in regulating the encryption software was not targeted to either the expressive content of the comments or the source code.[250] Rather, the government desired to decrease foreign intelligence ability to encode communications.[251] Karn, therefore, had the burden of proving bad faith or motive of the government, but he did not satisfy this burden.[252] The government satisfied the elements of the *O'Brien* test. The government had the authority to control the export of defense articles, the export regulation furthered an important governmental interest of preventing the "proliferation of cryptographic products," and the regulation was "'no greater than is essential to the furtherance of that interest.'"[253]

The parties agreed that the first two requirements of the test were met.[254] Karn argued that the last requirement had not been satisfied, pointing to the fact that the cryptographic algorithms were already

[243] *Id.*

[244] *Id.* at 9-14 (suggesting that the regulation was content-neutral and narrowly tailored to further the significant government interest of controlling the proliferation of cryptographic products).

[245] *Id.* at 9. Karn also stated a claim for violation of his Fifth Amendment rights, *id.* at 3, however, the Fifth Amendment analysis is beyond the scope of this Comment.

[246] The *Karn* court chose not to address the book's classification because the government only prohibited the export of the diskette. *Id.* at 9. Moreover, Karn did not question the book's classification before the court. *Id.*

[247] *Id.* at 9-10.

[248] *Karn*, 925 F. Supp. at 9-10. Notably, the court stated that it was not ruling as to whether the source code without comments is protected speech. *Id.* at 10. More importantly, the court did admit that source codes are "merely a means of commanding a computer to perform a function." *Id.* at 9 n.19.

[249] *Id.* at 10; *see supra* notes 178-86 and accompanying text.

[250] *Karn*, 925 F. Supp. at 10.

[251] *Id.* The government claimed, "the proliferation of [cryptographic hardware and software] will make it easier for foreign intelligence targets to deny the United States Government access to information vital to national security interests." *Id.* at 11.

[252] *Id.* at 10-11.

[253] *Id.* at 11 (citing United States v. O'Brien, 391 U.S. 367, 377 (1968)).

[254] *Id.*

available abroad at the time he requested a license jurisdiction.[255] In addition, the algorithms on the diskette at issue were so weak that the National Security Agency could break the codes.[256] The court rejected this argument, noting that the President placed cryptographic products on the ITAR to protect the United States from the potential harm caused by the proliferation of cryptographic products.[257] The court refused to judge this foreign policy decision.[258] The court also refused to review the harms created by the regulation and the injury to national security under the ad hoc balancing test of *Tinker v. Des Moines Independent Community School District*:[259] "[S]uch a test in the case at bar would require the Court to scrutinize the actual injury to national security."[260]

Interestingly, in *Karn*, there was no finding with respect to the "functionality" of the Karn diskette as a cryptographic device.[261] The court, however, acknowledged that the government's policy decision that "the proliferation of this type of product is harmful to the national security" was persuasive enough to uphold the regulation of the software.[262]

Finally, the *Karn* court found that the plaintiff did not present any support for the argument that the regulation was "'substantially

[255] *Id.* The court disagreed with Karn's contention that the third prong was in dispute. *Id.* Karn actually addressed the second prong, as the argument questioned whether the government had a legitimate interest at stake. *Id.*

[256] *Karn*, 925 F. Supp. at 11.

[257] *Id.*

[258] *Id.* ("[The President's] policy judgment exists despite the availability of cryptographic software through the Internet and the National Security Agency's alleged ability to break certain codes. Even if this were a factual dispute, it is not one into which this Court can or will delve."). The court supported this conclusion by citing the Supreme Court in *Chicago & Southern Air Lines v. Waterman Steamship Corp.*, 333 U.S. 103, 111 (1948) (proposing that the President's foreign policy decisions are the responsibility of the Executive branch and that the Judiciary has "neither aptitude, facilities nor responsibility"). *Karn*, 925 F. Supp. at 11.

[259] 393 U.S. 503 (1969).

[260] *Karn*, 925 F. Supp. at 12; *see* United States v. Mandel, 914 F.2d 1215, 1223 (9th Cir. 1990) ("[W]hether the export of a given commodity would make a significant contribution to the military potential of other countries . . . is a political question not subject to review to determine whether [it] had a basis in fact."); United States v. Martinez, 904 F.2d 601, 602 (11th Cir. 1990) ("The question whether a particular item should have been placed on the Munitions List possesses nearly every trait that the Supreme Court has enumerated traditionally renders a question 'political.'").

[261] *Karn*, 925 F. Supp. at 12. In *Bernstein v. United States Department of State*, 974 F. Supp. 1288 (N.D. Cal. 1997), the government argued that the export of encryption software and other encryption products must be controlled because of its functional capacity, rather than any informational value the software provides. *Id.* at 1305; *see supra* text accompanying note 72 (proposing that the government's purpose is to control software because of its functionality, not because of its possible expression).

[262] *Karn*, 925 F. Supp. at 12.

broader than necessary'" to achieve the government's stated objective.[263] Furthermore, Karn did not provide any proof of current barriers to distributing the information relating to cryptography by any available alternative means other than the export of encryption source code on machine-readable media.[264]

B. Bernstein v. United States Department of State

Less than one month after the *Karn* court decided and filed its opinion holding source code was constitutionally regulated, the Northern District of California found source code constituted protected speech.[265] Six months later on cross-motions for summary judgment, Judge Patel held that the government licensing scheme created an unlawful prior restraint on speech.[266] In 1997, Bernstein filed an amended complaint in response to an executive order transferring jurisdiction over commercial encryption exports from the State Department to the Commerce Department.[267] The court in this most recent decision held that Bernstein failed to establish a statutory challenge to the executive order, that the government regulations remained subject to a prior restraint analysis, and that the licensing scheme imposed on

[263] *Id.* (citing Members of City Council v. Taxpayers for Vincent, 466 U.S. 789, 808 (1984)).

[264] *Id.* (citing Clark v. Community for Creative Non-Violence, 468 U.S. 288, 295 (1984)).

[265] Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996) [hereinafter *Bernstein I*]. In his first complaint, Bernstein sought declaratory and injunctive relief from enforcement of the AECA and ITAR. *Id.* at 1428. The district court found that source code was protected by the First Amendment. *Id.* at 1436. The court made no final judgment on the merits, but did find that the plaintiffs presented a colorable and justiciable constitutional challenge. *Id.* at 1439. As the *Karn* court considered the regulating issue as the government's interest in protecting national security and *Bernstein* viewed the issue as one of speech suppression, *Bernstein I* became the first opinion recognizing computer code as protected speech. *See* Thinh Nguyen, *Cryptography, Export Controls, and the First Amendment, in* Bernstein v. United States Department of State, 10 HARV. J.L. & TECH. 667, 672 (1997). "[T]he issue was transformed from the realm of the government's interest in controlling the export of material deemed harmful to national security, or a 'political question' in *Karn*, to the right to speak cryptographically in *Bernstein*." Stender, *supra* note 2, at 315.

[266] Bernstein v. United States Dep't of State, 945 F. Supp. 1279, 1290 (N.D. Cal. 1996) [hereinafter *Bernstein II*]. In *Bernstein II*, the court found parts of the scheme unconstitutionally vague while upholding other parts as constitutionally sufficient. *Id.* at 1292-95. The court concluded that the ITAR licensing requirements for encryption software constituted an unlawful prior restraint. *Id.* at 1290. The government argued that the restraint was a justified means of ensuring national security. *Id.* at 1288. The court found that the national security reasoning alone did not justify the restraint. *Id.* ("[N]ational security, without more, [is] too amorphous a rationale to abrogate the protections of the First Amendment.") (citing New York Times Co. v. United States, 403 U.S. 713, 730 (1971)).

[267] Bernstein v. United States Dep't of State, 974 F. Supp. 1288, 1292 (N.D. Cal. 1997) [hereinafter *Bernstein*].

encryption software acted as an unconstitutional prior restraint of protected speech.[268]

Professor Bernstein developed an encryption algorithm while he was a graduate student at the University of California at Berkeley.[269] He articulated the algorithm in an academic paper both in English and in "source code" high-level computer programming language.[270] In 1992, Bernstein submitted to the State Department[271] a commodity jurisdiction request[272] with regard to his "Snuffle" encryption algorithm.[273] The State Department informed Bernstein that "Snuffle" was a defense article under the ITAR and could not be exported without a State Department license.[274] Bernstein filed suit, claiming the AECA and the ITAR restricted his ability to teach, publish or discuss his theories on cryptography as referred to in his program. Bernstein argued that the licensing requirements constituted a prior restraint on his right to free speech in violation of the First Amendment.[275]

On August 25, 1997, the court agreed with Bernstein, finding the regulations presented "a danger of unduly suppressing protected expression."[276] The court reasoned that "[w]hile defendants may have the authority to regulate encryption source code, they must nonetheless do so within the bounds of the First Amendment."[277] The Supreme Court requires a presumption against the constitutional validity of prior restraints.[278] The government, according to the *Bernstein* court, failed to rebut the presumption.[279]

[268] *Id.* at 1300-09. The government appealed the final *Bernstein* ruling. *Does Constitution Protect Software as Free Speech? Federal Court Rejects Argument in Challenge of U.S. Regulations*, STAR-TRIB., Aug. 2, 1998, at 6D, *available in* 1998 WL 6362983 [hereinafter *Does Constitution Protect*]. The parties argued before the Ninth Circuit Court of Appeals and are now awaiting decision. *Id.*

[269] *Bernstein I*, 922 F. Supp. at 1428-29.

[270] *Id.* at 1429. See *supra* notes 33-46 and accompanying text for a discussion of source code.

[271] This submission, in 1993, occurred when the State Department still had jurisdiction over commercial encryption exports, and such exports were governed by the ITAR. *Bernstein*, 974 F. Supp. at 1288. See *supra* notes 68-71 for a discussion of the transfer of control from the State Department to the Commerce Department.

[272] See *supra* note 79 for a description of the commodity jurisdiction request process.

[273] *Bernstein I*, 922 F. Supp. at 1430. "Snuffle" is the name Bernstein chose to call his program. *Id.*

[274] *Id.*

[275] *Bernstein*, 974 F. Supp. at 1293. Bernstein also argued that various terms make the regulation vague and overbroad in violation of the First Amendment. *Id.* at 1296. Furthermore, he complained that the regulations violated his freedom of association. *Id.* These complaints will not be addressed in this Comment.

[276] *Id.* at 1306 (citing Freedman v. Maryland, 380 U.S. 51, 54 (1965)).

[277] *Id.* at 1303.

[278] Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971); *see supra* notes 217-18 and accompanying text.

[279] *Bernstein*, 974 F. Supp. at 1308.

The court found that the encryption regulations were directed to "an entire field of applied scientific research and discourse."[280] It reasoned that cryptographic software may be exported subject to the regulation for non-expressive reasons.[281] Scientists, however, may in fact develop and use cryptographic software programs for expressive reasons while remaining subject to the licensing requirements.[282] With this, the court argued, the regulation acted as a prior restraint suppressing constitutionally protected expression.[283]

The court also found the exception for printed materials "irrational and administratively unreliable."[284] The court cited *Reno v. American Civil Liberties Union*[285] for the proposition that electronic media and print media should be reviewed under the same degree of strict scrutiny.[286] Therefore, the government could not rationally treat materials with varying levels of review simply because they were carried by different mediums.[287]

With regard to the government's national security concerns, the court determined these alone were not enough to justify a prior restraint on speech.[288] The court, citing Justice Brennan in *New York Times Co. v. United States*,[289] concluded that prior restraints under the First Amendment could only be upheld during a time of war.[290] Such restraints must prevent "direct, immediate, and irreparable damage to our Nation or its people."[291] According to *Bernstein*, the President and the BXA justified the regulation as protecting interests of na-

[280] *Id.* at 1305.

[281] *Id.*

[282] *Id.* (demonstrating expressive activities such as teaching, publishing, speaking, or Internet communications).

[283] *Id.* at 1308.

[284] *Id.* at 1306 (noting that the regulations allow for the international export of written materials in a book without a license, yet the same information on a disk and exporting it internationally is subject to the export regulations' licensing requirements).

[285] 117 S. Ct. 2329, 2344 (1997) (suggesting that distinguishing between written and electronic media is unjustified and that the Internet is subject to the same constitutional scrutiny as print media).

[286] *Bernstein*, 974 F. Supp. at 1306-07. The court also noted that distinguishing between written and electronic transmission is dangerous in an age where many professional journals are converted to electronic form onto the Internet. *Id.* at 1306.

[287] *Id.* at 1307.

[288] *Id.*

[289] 403 U.S. 713, 726 (1971) (Brennan, J., concurring) (citing Schenck v. United States, 249 U.S. 47 (1919)).

[290] *Bernstein*, 974 F. Supp. at 1307.

[291] *New York Times Co.*, 403 U.S. at 730 (Stewart, J., & White, J., concurring).

tional security and foreign policy.[292] These interests, according to the court, were insufficient to justify a prior restraint on speech.[293]

The *Bernstein* court also noted that a regulation did not have to be aimed at the content to be a prior restraint on speech.[294] The fact that the regulation was directed at "expressive activity" was sufficient to apply the prior restraint test.[295] Thus, the court held that even a licensing regulation with a content-neutral purpose must adequately provide constitutional procedural safeguards.[296] According to *Bernstein*, the adequacy of the safeguards are then reviewed by the *Freedman* test.[297]

Applying the *Freedman* test, the court concluded that the licensing scheme was unconstitutional.[298] First, the court found that the licensing scheme did not provide for a specific time period within which applications would be decided.[299] The scheme does not restrict the time for the government to make a licensing decision.[300] The only time restriction applied to the appeal process, and this restriction vaguely required that an appeal be made within a reasonable time.[301] Second, the court held the licensing scheme prohibited judicial review of the agency's appellate decision.[302] Finally, the government had not stipulated to any standards for deciding an application.[303] The government's proposed case-by-case analysis, arguably without any limits, did not satisfy the third requirement in *Freedman*: "[T]he censor must bear the burden of going to court to uphold a licensing denial and once there bears the burden of justifying the denial."[304]

In sum, the district court agreed with the plaintiff that a computer program consists of more than a process to operate a computer, and truly forms a medium for the expression of ideas.[305] Furthermore, the

[292] *Bernstein*, 974 F. Supp. at 1307.

[293] *Id.* Notably, the court conceded that it remains unclear what the Supreme Court standard is for finding justification of a prior restraint. *Id.*

[294] *Id.*

[295] *Id.*

[296] *Id.*

[297] *Id.*

[298] *Bernstein*, 974 F. Supp. at 1307.

[299] *Id.* at 1308. See *supra* notes 78-84 for a discussion of the licensing application process and procedures.

[300] *Bernstein*, 974 F. Supp. at 1308.

[301] *Id.*

[302] *Id.*

[303] *Id.*

[304] *Id.*

[305] *Id.* at 1305 ("[T]he court does not disagree that encryption software is highly functional, but functionality does not remove it from the realm of speech. Just because an idea is functional does not 'negate' its expressiveness. Indeed, it is functional speech.").

court found that the encryption regulation did not provide adequate procedural safeguards.[306] Therefore, the *Bernstein* court ruled that the government regulation violated the First Amendment as a prior restraint on speech.[307]

Contrary to *Karn*, the *Bernstein* court applied the *Freedman* prior restraint test to the governmental regulation of encryption software.[308] The court did not find that defining the regulation as content-based or content-neutral was necessary. The court simply held that the government regulation unconstitutionally restrained protected speech.[309]

V. Analysis

A. *Is Cryptographic Software Speech?*

In *Bernstein I*, the court held that computer software was pure speech protected by the First Amendment.[310] This court rejected the proposition that software was merely functional, comprising "no original speech expression in and of itself,"[311] and thus removed from the confines of the First Amendment.[312] Rather, the court analogized source code to various forms of "[i]nstructions, do-it-yourself manuals, recipes, even technical information about hydrogen bomb con-

[306] *Bernstein*, 974 F. Supp. at 1308. ("The new regulations, . . . are woefully inadequate. . . . [T]here is no time limit on an application that has been referred to the President. . . . [M]ost lacking, are any standards for deciding an application.").

[307] The court limited its August holding so that it applied only to Professor Bernstein and his "Snuffle" algorithm. *Id.* at 1310. On December 8, 1997, however, the government appealed the ruling to the Ninth Circuit Court of Appeals. *Does Constitution Protect*, *supra* note 268. According to the reports of the oral arguments, the judges appeared skeptical of the government's arguments in support of encryption controls. John Markoff, *Court Hears Appeal in Encryption Case*, N.Y. Times, Dec. 9, 1997, at D5. According to Stewart Baker of Steptoe & Johnson, regardless of the skepticism, it is unlikely that the Ninth Circuit will strike down all export controls. Stewart Baker, *Ninth Circuit Hearing In The Bernstein Case*, Mondaq Bus. Briefing, Jan. 13, 1997 (visited Nov. 10, 1998) <http://www.mondaq.com/docs/mainbody/1006257.html>. If the court does find in favor of Bernstein, its holding will likely be narrowly tailored. *Id.* In any case, any decision against the government almost certainly will be appealed to the Supreme Court. *Id.* The circuit court is expected to make a decision soon. Jon Swartz, *Appeals Court Hears Encryption Software Case*, S.F. Chron., Dec. 9, 1997, at C1.

[308] *See supra* notes 296-303 and accompanying text.

[309] *See supra* notes 305 and accompanying text.

[310] Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1436 (N. D. Cal. 1996); *see supra* note 263 and accompanying text. The court erred by simply stating software was speech because it was protected by copyright law. *Bernstein*, 922 F. Supp. at 1436. The court failed to mention that patent law protects software as well. Copyright protects expression, while patent law protects machines, processes, and tools. *Id.* Although this debate is relevant, it is too extensive for this Comment.

[311] Stender, *supra* note 2, at 316.

[312] *Bernstein*, 922 F. Supp. at 1435.

struction."[313] However, this analogy is flawed. Unlike these written instructions intended to be read, understood, and followed by humans, source code acts as a machine that actually carries out the function intended and as a tool that creates speech,[314] similar to how pens and paper aid the writer to express ideas. Proposing the pen and paper are truly the resulting speech is dubious at best.

More importantly, failing to acknowledge cryptography as "a technology that transforms communication between parties and makes no original speech expression in and of itself"[315] creates problems of its own. "It is particularly ill-suited to the realities of computer technology because software inseparably incorporates elements of both expression and function."[316] Cryptography simply lacks the expressive element required to summon the protections of the First Amendment. "A critical insight into the First Amendment protection of speech is that it attaches not to particular *things* or types of *objects* (such as computer source code) but to *activities* where the free exchange of information and ideas is at stake (such as publishing and giving a speech)."[317]

The *Karn* court explicitly stated, "source codes are merely a means of commanding a computer to perform a function."[318] The court's analysis, however, conceded that source code and its comments are protected speech.[319] The court failed to analyze the probability that the comments themselves were not speech.[320] If in fact software is not speech, the government regulation is not unconstitutional on First Amendment grounds.

[313] *Id.* (citing United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979)).

[314] See *supra* notes 34-40 and accompanying text.

[315] Stender, *supra* note 2, at 316. *See* Nguyen, *supra* note 265, at 677 (proposing that "[t]he problem with the [*Bernstein*] court's analysis is that it focuses too narrowly on the nature of computer source code, rather than looking to the larger social context surrounding the regulated activities in which software plays a part").

[316] Nguyen, *supra* note 265, at 675-76.

[317] *Id.* at 677-78.

[318] Karn v. United States Dep't of State, 925 F. Supp. 1, 9 (D.D.C. 1996). The Court withheld any judgment regarding whether or not source code without comments are protected by the First Amendment. *Id.* at 9 n.19.

[319] *Id.* at 9. "Assuming the source codes and comments are within the arena of protected speech, the Court must then determine the basis for the regulation at issue in this case." *Id.* at 10.

[320] It is not at issue whether or not object code is speech because this code is simply numbers for only the computer to interpret. *See supra* note 38 and accompanying text. The object code is not human readable. *See supra* notes 38-40 and accompanying text. The issue revolves around source code and its accompanying comments. The *Karn* court implied that source code without comments would not classify as speech. *Karn*, 925 F. Supp. at 10 n.19. At issue, then, is whether or not software with comments is speech. Therefore, for purposes of this analysis, "software" and "source code" implies that author-written comments are included.

As a computer program, software enables one machine to perform the functions of many machines.[321] "When a word processing program is operating in a computer, the computer is a word processor. When a videogame program is operating in a computer, the computer is a videogame machine. When a digital watch program is operating in a computer, the computer is a digital watch."[322] When an encryption software program is operating in a computer, the computer is a cryptographer. A computer program makes a new machine structure. By the classical definition, a machine is a set of devices configured to perform a specific function;[323] "'one employs motors, levers, gears, and wire to print newspapers; another uses motors, levers, gears, and wire to play a prerecorded song.'"[324]

A computer is also made by configuring a set of devices, but its function is not implied by that configuration. It acquires its function only when someone programs it.[325] This program is in turn called software.[326] Proponents of "software is speech" would not suggest that the "motors, levers, gears and wires" creating a newspaper is speech protected by the First Amendment. The same proponents would not propose that the "motors, levers, gears, and wire" are speech when operating to play a song. The proponents of "software is speech," however, continue to argue that a software program is speech when functioning to create a cryptographic machine.[327] Since World War II, machines have been transformed though programming.[328] For example, the ENIAC,[329] the first general-purpose electronic computer, was manually programmed using wiring and mechanical switches to decipher coded German communications during the war.[330] The attaching of cables made new circuitry, i.e., a spe-

[321] Samuelson, *supra* note 21, at 680.

[322] *Id.*

[323] *See supra* notes 25-30 and accompanying text.

[324] James R. Goodman et al., *The* Alappat *Standard for Determining that Programmed Computers are Patentable Subject Matter*, 76 J. PAT. & TRADEMARK OFF. SOC'Y 771, 782 (1994) (quoting Paul Ceruzzi, *An Unforseen Revolution: Computers and Expectations, 1935-1985*, *in* IMAGINING TOMORROW: HISTORY, TECHNOLOGY, AND THE AMERICAN FUTURE 187, 196 (Joseph J. Corn ed., 1986)).

[325] *See supra* notes 29-33 and accompanying text.

[326] *See supra* notes 29-33 and accompanying text.

[327] *See supra* notes 246-48, 275-77 and accompanying text.

[328] Goodman et al., *supra* note 324, at 773.

[329] *See supra* note 24.

[330] *See* CHARLES BASHE ET AL., IBM'S EARLY COMPUTERS, 1-33 (1986); Arthur W. Burks & Alice R. Burks, *The ENIAC: First General Purpose Computer*, ANNALS HIST. COMPUTING 310 (1981); *see also* Ceruzzi, *supra* note 324, at 189 (showing a photograph of the ENIAC programming). "This rewiring essentially changed it into a new machine for each new problem it solved." *Id.* at 196.

cial purpose computer, thereby transforming the ENIAC into a decoding machine.[331] Just as the wiring and mechanical switches that created the decoding machine were not speech then, the encryption software that creates the cryptography machines is not speech today.

B. *Is "Cryptographese" Protected Speech?*

If the courts determine encryption source code is speech, it is not speech protected by the First Amendment. The Supreme Court clearly asserted that not all speech remains protected by the First Amendment.[332] Speech receives or loses protection based in part on its determined value.[333] Categorizing software and its source code will assist in determining its constitutional value. Concededly, the categorical characteristics are not clear.[334] Applying consistently recognized Supreme Court categories confirms the conclusion that software cannot be protected under the First Amendment.

First, source code is not high-value political speech.[335] In *New York Times v. Sullivan*,[336] the Court found compelling the need to encourage statements, even if false or erroneous statements, in the interest of promoting free debate.[337] Encryption source code does not promote the "debate on public issues,"[338] or "sharp attacks on government"[339] or any other political figure. Moreover, it does not encourage "free flow of information and opinion about matters of public concern [which] is essential to effective self-government."[340] Simply stated, source code is not "core" value speech.[341] At best, software remains a "lower-valued" classification of speech.[342]

[331] *See supra* note 24 and accompanying text.

[332] *See supra* note 106 and accompanying text.

[333] *See* Shaman, *supra* note 107, at 298.

[334] *See supra* note 116 and accompanying text.

[335] *See* Shaman, *supra* note 107, at 333 (restating Alexander Meiklejohn's view of the central purpose of freedom of speech). "[T]he central purpose of freedom of speech and the press is to enable individuals to participate in our democratic system of self-government." *Id.*

[336] 376 U.S. 254 (1964). See *supra* note 120 for the factual background of *Sullivan* and the Supreme Court's reasoning for protecting the political speech.

[337] *Sullivan*, 376 U.S. at 270; *see supra* notes 119-21 and accompanying text.

[338] *Sullivan*, 376 U.S. at 270; *see supra* text accompanying note 121.

[339] *Sullivan*, 376 U.S. at 270.

[340] Shaman, *supra* note 107, at 333. Arguably, source code comments could include such expressions. The proliferation of political speech, however, is not the intended use of source code, nor is source code currently utilized for such a purpose. Notably, even if source code did include political speech, the government regulations would pass constitutional muster because of the harm it caused, *see supra* notes 42-44 and accompanying text, and because of its ability to satisfy the *O'Brien* test, *see infra* Part V.C.

[341] *See* GUNTHER, *supra* note 108, at 999-1002 (discussing various approaches to valuing speech).

[342] *See supra* notes 131-36 and accompanying text.

Clearly, speech does not have to be political to warrant First Amendment protection. Yet, software does not warrant protection under a less protected category. For example, commercial speech is protected by the First Amendment, albeit to a lesser degree than political speech.[343] Computer software does not promote a commercial transaction, which is granted an intermediate level of protection.[344] Neither source code nor its accompanying comments function as an advertisement, mention a specific product by name, or are created with economic motivations.[345] The software developer may write code with a partial objective of financial gain. The third factor, economic motivation, is not satisfied simply by the placement of a price tag. If this were true, arguably every textbook mentioning a product would be classified as commercial speech. Thus, computer software does not satisfy the elements defining commercial speech.

Lastly, encryption software does not even qualify for protection as low-value speech, which warrants some protection by the First Amendment.[346] The government should be able to regulate some activities accomplished through speech.[347] Professor Frederick Schauer explains that "[n]ot only do we fix prices with speech, but we also make contracts with speech, . . . extort with speech, threaten with speech, and place bets with speech."[348] These activities do not present a clear and present danger, nor does the government have a particularly compelling interest in prohibiting them.[349] Their constitutional governmental regulation, therefore, can only be explained under the low-value speech theory. These classes of speech "are to be tested under drastically different standards of protection" than other speech afforded greater First Amendment value.[350]

Assuming for argument's sake that software is afforded minimal protections as low-value speech, cryptographic software is one form of speech the government should be able to regulate. Software is not

[343] Shaman, *supra* note 107, at 319; *see supra* notes 122-30 and accompanying text.

[344] Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations, 413 U.S. 376, 385 (1973) (holding a mere proposal of possible employment is not protected by the First Amendment); *see* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976) (holding a statute making it illegal to advertise prescription drug prices an unconstitutional violation of protected commercial speech).

[345] See *supra* text accompanying note 121 for a detailed list of factors the Court considers characteristic of commercial speech.

[346] *See* Sunstein, *supra* note 157, at 602.

[347] Frederick Schauer, *Categories and the First Amendment: A Play in Three Acts*, 34 VAND. L. REV. 265, 270-72 (1981).

[348] *Id.* at 270.

[349] *Id.* at 271.

[350] *Id.* at 271-72.

worthless in the sense of its functionality, but its alleged expressive content is "worthless or of de minimis value to society."[351] Society generally is not concerned with what the software is communicating to the computer or what the source code comments convey to a reader.[352] The concern is simply that the software does what it is supposed to do.[353]

Classified as low-value speech, cryptographic software is worthy of only minimal scrutiny.[354] The government, therefore, need only establish a "valid or legitimate state interest achieved through reasonable means."[355] There is a legitimate state interest in national security.[356] The licensing regulation of encryption is a reasonable means of achieving such an interest.

Opponents to cryptography controls argue that criminals have international means of obtaining strong encryption technology and therefore the United States government need not enforce export restrictions. This reasoning, however, does not justify further proliferation through United States channels.[357] J. Terrence Stender, former United States Navy cryptologist and signals intelligence situation analyst, suggested that the United States should restrict the export of encryption, as well as any other military-related technology regardless of its availability from foreign suppliers.[358] Stender poses a variety of rhetorical questions on this proposition worthy of serious consideration: "Should the United States allow the export of sophisticated mis-

[351] R.A.V. v. St. Paul, 505 U.S. 377, 400 (1992).

[352] *See* Samuelson, *supra* note 21, at 682; *see supra* notes 40-46 and accompanying text.

[353] *See supra* notes 40-42 and accompanying text.

[354] Shaman, *supra* note 107, at 330.

[355] *Id.*

[356] *See supra* Part II.C.

[357] *See* Stender, *supra* note 2, at 322. *But see* United States v. Progressive, Inc., 610 F.2d 819 (7th Cir. 1979). On March 26, 1979, the Wisconsin district court issued a preliminary injunction prohibiting the publication of Howard Morland's article on how to build a hydrogen bomb pursuant to the Atomic Energy Act, 42 U.S.C. § 2280. United States v. Progressive, Inc., 467 F. Supp. 990, 996 (W.D. Wis. 1979). The court further held that even in the absence of the Atomic Energy Act, the injunction would be justified as a means of preventing irreparable harm to the United States. *Id.* The government's suit was dismissed while pending before the Seventh Circuit, however. *Progressive*, 610 F.2d at 819. Professor Stone believes that the dismissal occurred because other writers published materials providing similar instructions. Stone, *supra* note 157, at 1034. I would like to thank Professor Rodney Blackmun for his insight on the *Progressive* case.

[358] Stender, *supra* note 2, at 322 (citing U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, EXPORT CONTROLS AND NONPROLIFERATION POLICY O.T.A.-ISS-596, 56 (1994)).

> While it is recognized that a significant number of encryption programs are already available from non-U.S. sources worldwide, and in many cases obtained quite cheaply and easily, it would appear not to be in the best interests of the United States, as a pure security matter, to contribute to the proliferation of encryption.

Id.

sile technology, just because it just so happens that the Chinese and the Russians have similar systems available on the open market? . . . Why help an already bad situation get worse?"[359] Arguing the elimination of export controls on cryptography simply because it is available in foreign nations is analogous to encouraging the elimination of drug enforcement simply because drugs are available through international suppliers.

As mentioned earlier, the government perceives the proliferation of encryption technology as a harmful threat to national security.[360] Applying the definitional balancing approach to this form of low-value speech, the courts may uphold the federal export regulation upon finding the proliferation of encryption software harmful.[361] The court does not have to find actual harm.[362] Finding speech threatens the exposure of United States coding systems to foreign intelligence, thereby causing loss of control and secrecy of United States government codes and confidential information, and arming foreign terrorists with a tool to carry out attack missions,[363] is enough evidence to establish harmful speech. Even under the low-value speech theory, therefore, encryption software does not violate the First Amendment.

The government encryption export regulations have also been challenged as an unconstitutional prior restraint on speech.[364] The Supreme Court in *City of Lakewood v. Plain Dealer Publishing Co.* required a finding of a "close enough nexus to expression or to conduct commonly associated with expression" to invalidate a prior restraint.[365] Encryption software has little expressive value.[366] Moreover, the software is not "commonly associated with expression."[367] "Software . . . empowers a computer to handle information and to control information flow,"[368] and is commonly distributed for its non-expressive purposes of providing a compiler with enough information to produce executable computer programs.[369] Additionally, for a law to be invalidated as a prior restraint, the Court must be

[359] *Id.*

[360] *See supra* Part II.C.

[361] *See supra* text accompanying notes 164-67 (noting that definitional balancing applies to low-value speech).

[362] *See* Shaman, *supra* note 107, at 331.

[363] *See supra* Part II.C.

[364] *See* Bernstein v. United States Dep't of State, 974 F. Supp. 1288, 1296 (N.D. Cal. 1997).

[365] City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 759 (1988); *see supra* notes 227-30 and accompanying text.

[366] *See supra* text accompanying notes 41-47, 310-31.

[367] *Lakewood*, 486 U.S. at 760-61.

[368] STOBBS, *supra* note 30, at 50.

[369] *Id.* at 170.

persuaded that the regulated conduct offers more than a mere possibility of expressive nature.[370] Exporting encryption software may at times be exported for expressive reasons. Regardless, more than a mere possibility is required. Simply because exporting software may on occasion be expressive is not enough to implicate the prior restraint doctrine.

The Supreme Court applies the categorization approach to assessing levels of protection on speech. Other justifications have been proposed in support of the First Amendment freedom of speech, such as the creation of an open marketplace of ideas and promoting self-development.[371] Software does not liken to any of these categories. Computer scientists consider source code comments a kind of "marginal note" the programmer makes to himself.[372] The comments by no means facilitate the "marketplace of ideas"[373] or promote self-development. They are not statements critical of the government[374] or any other subject of public debate. In fact, it has been said that the user does not care what the program says, as long as it "does what it is supposed to do."[375]

As Professor Alexander Meiklejohn observed, the First Amendment does not prohibit the abridging of speech, but abridging the freedom of speech.[376] "The values perceived in a system of free expression will be determinative of whether there exists an inhibition upon that freedom."[377] In sum, the values and functions of freedom of expression are numerous. "First, freedom of expression is essential as a means of assuring individual self-fulfillment. . . . [Second, it] is an essential process for advancing knowledge and discovering truth. . . . [Third, it] is essential to provide for participation in decision making by all members of society."[378] Computer software does not facilitate any such functions.

[370] *See* Roulette v. City of Seattle, 97 F.3d 300, 303 (9th Cir. 1996) (finding sitting on sidewalks as not subject to facial prior restraint challenge even though sitting on city sidewalks may at times be expressive); *see supra* Part III.E.

[371] LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-1, at 785-88 (2d ed. 1988).

[372] Samuelson, *supra* note 21, at 685.

[373] *See supra* note 121 and accompanying text.

[374] *See supra* note 121 and accompanying text.

[375] Samuelson, *supra* note 21, at 682.

[376] ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF GOVERNMENT 19 (1948) ("The First Amendment is not the guardian of unregulated talkativeness.").

[377] NOWAK & ROTUNDA, *supra* note 105, at 940.

[378] THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 6-7 (1970).

C. *Is Encryption Expressive Conduct?*

If the court finds encryption software is speech, it should only afford limited protection as expressive conduct.[379] Conceding for argument's sake that the encryption source code contained on a disk is speech, the government is suppressing the conduct of encryption with an element of speech. The government does not regulate the encryption conduct because of its expressive value, as it does not restrict the export of the encryption process because of the expressive message the software may include. Instead, the government regulates the export of encryption software simply to protect national security. Any impact on expression is incidental to "permissible export controls on a commodity that can function to encrypt communications."[380] Accordingly, the Supreme Court has held that where the government suppresses speech incidental to conduct, the content-neutral regulation is not per se unconstitutional and *O'Brien* applies.[381]

The *Karn* court correctly found that the government satisfied all elements of the *O'Brien* test.[382] It has been conceded that the government had the authority to regulate the export of defense articles.[383] Also, whether the governmental has a substantial interest in protecting critical foreign intelligence is not at issue.[384] The third element required the encryption software controls to be unrelated to the suppression of speech.[385] As stated in *Karn*, the government in the encryption regulation cases correctly argued that "[t]he encryption source codes on [the] disks are not regulated because of any scientific ideas that are implicit in them. The focus of the regulation is on the function of a commodity."[386]

[379] In *O'Brien*, the government constitutionally prohibited the *act* of destroying draft cards. United States v. O'Brien, 391 U.S. 367 (1968). The government's purpose was unrelated to regulating pure, free speech, but intended to ensure that the draft cards were made available for government tracking purposes. *Id.* at 378-82. Similarly, the government is now regulating the *act* of strong encryption processes without key recovery systems. The government's purpose is unrelated to regulating pure protected speech. *See supra* text accompanying note 72. The act of encryption happens to be in the form of a diskette. Notably, the form of the expression is irrelevant if the government's interest is unrelated to suppressing free speech. *O'Brien*, 391 U.S. at 377.

[380] Memorandum of Points and Authorities in Support of Defendant's Motion to Dismiss, or in the alternative, For Summary Judgment at 5, Karn v. United States Dep't of State, 925 F. Supp. 1 (D.C.C. 1996) (visited Oct. 19, 1997) <http://people.Qualcomm.com/karn/export/memorandum.html>.

[381] United States v. O'Brien, 391 U.S. 367, 376 (1968).

[382] Karn v. United States Dep't of State, 925 F. Supp. 1, 12 (D.D.C. 1996).

[383] U.S. Const. art. I, § 8.

[384] *See supra* Part II.C.

[385] *O'Brien*, 391 U.S. at 377.

[386] Defendant's Motion at 5, *Karn*.

Arguably, it is the fourth element, requiring narrowly tailored means, that has caused much of the controversy. The government restricted the export of encryption source code on disk, yet it does not restrict the export of source code in written form.[387] This is justified, however, because the government does not desire to completely suppress the international sharing of encryption code.[388] Rather, the government merely regulates the form of the code that can be exported to foreign nations.[389] Therefore, regulating the code in disk form and not in print limits the suppression of alleged First Amendment freedoms. The incidental restriction on the alleged First Amendment freedoms is "no greater than is essential to the furtherance of" ensuring national security.[390]

D. Separation of Powers

The government regulations on encryption software as a means of ensuring national security raises the question of a proper separation of powers. This doctrine dictates that

> [T]he scope of the judicial function on passing upon the activities of the Executive Branch . . . in the field of foreign affairs is very narrowly restricted. . . . [In this limited power,] the judiciary must review the initial executive determination to the point of satisfying itself that the subject matter of the dispute does lie within the proper compass of the President's foreign relations power. . . . [T]he judiciary may properly insist that the determination that disclosure of the subject matter would irreparably impair the national security be made by the head of the Executive Department concerned [after] actual personal consideration by that officer.[391]

[387] *Karn*, 925 F. Supp. at 5.

[388] *See supra* notes 78-87 and accompanying text.

[389] *See supra* notes 78-87 and accompanying text. The government reasonably believes that the threat to national security derives from providing foreign programmers with the actual encryption code in functional form. The written form does not pose the same threat of use, unlike the disk. The written form requires manipulation and manual labor to effectuate the process. The process of converting the software from written form into a usable electronic form increases the risk of errors in the program. If in fact the conversion program contains errors, or bugs, the encryption process will fail to operate as the likelihood of collecting bugs in a program is great and the time to locate and correct bugs is extensive. *See* Samuelson, *supra* note 21, at 686-87 (stating that "[t]o locate the source of the errors and to correct them almost takes longer than writing the source code"). Arguably software source code in written form is less threatening to security than executable code on an operational diskette. *But see* Interview with Edward Apell, *supra* note 60 (suggesting that the wide distribution of encryption in either book or disk form is a national security threat as the book can be scanned into the computer and run to instruct the computer what to do, thus acting as the machine that it was meant to be).

[390] *Karn*, 925 F. Supp. at 11-12 (noting that the plaintiff had not articulated any present barrier to the spreading of information on cryptography "by any other means" other than those containing encryption source code on machine-readable media).

[391] New York Times v. Sullivan, 403 U.S. 713, 758 (1971) (Harlan, J., dissenting).

According to Justice Harlan's dissent in *New York Times v. Sullivan*,[392] however, "the judiciary may not properly go beyond these two inquiries and re-determine for itself the probable impact of disclosure on the national security:"[393]

> The very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments. . . . They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry.[394]

The government regulations on encryption software remain subject to Justice Harlan's above criticism. The judiciary has attempted to restrain the Executive Branch from enacting legislation with the purpose of protecting national security. In fact, the *Karn-Bernstein* line of cases "present[ ] a classic example of how the courts today, particularly the federal courts, can become needlessly invoked, whether in the national interest or not, in litigation involving policy decisions made within the power of the President or another branch of the government."[395]

VI. Impact

A. *Constitutional Impact*

On July 2, 1998, approximately two years after *Karn* and *Bernstein*, the United States District Court for the Northern District of Ohio filed its first encryption software opinion.[396] The court addressed whether encryption source code was expression protected under the First Amendment, whether the Export Regulations acted as a prior restraint on speech subject to heightened First Amendment scrutiny, and if not, whether the regulations survived intermediate scrutiny.[397] Finding the Export Regulations constitutional, the court reasoned that encryption source code is inherently functional, the regulations were not directed at source code's expressive elements, and the Export

[392] 403 U.S. 713 (1971) (Harlan, J., dissenting).

[393] *Id.* at 757.

[394] *Id.* at 757-58 (citing Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948)).

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

[396] Junger v. Daley, 8 F. Supp. 2d 708, 708 (N.D. Ohio 1998).

[397] *Id.* at 711-12.

Regulations did not apply to printed software or academic discussions of software.[398]

Junger filed a complaint against the Department of Commerce in the Northern District Court of Ohio.[399] He claimed, as did Karn and Bernstein, that the government regulations on encryption export violated his First Amendment rights.[400] Notably, however, unlike the complaints in *Bernstein* and *Karn*, Junger did not challenge per se the constitutionality of the licensing scheme's requirement of obtaining a license before exporting cryptographic devices. Instead, he argued that to require a license before one could communicate information violated the Constitution.[401]

Plaintiff Junger was a law professor at Case Western Reserve University Law School in Cleveland, Ohio.[402] He maintained a web site on the Internet that provided information about his courses to be read or downloaded.[403] He also wanted to publish his course book, articles, and other material on computers and the law, but these materials contained encryption software.[404] The government required Junger to obtain a license for his materials containing encryption code.[405] This requirement, Junger claimed, acted as a prior restraint in violation of the First Amendment.[406]

[398] *Id.* at 712.

[399] *Id.* at 711.

[400] *Id.* Junger taught a course in 1996, "Computers and the Law." *Id.* at 713. In addition to teaching his course, Junger created a web site for teaching and enabling anyone interested in his courses and topics to visit. *Id.* at 713-14. As a result of the transfer of encryption control to the Department of Commerce, Junger inquired whether his teaching, research or publication in his book and/or on his web site would be affected. *Id.* at 714. The government confirmed that the licensing requirement applied to specific items. *Id.* Junger applied for commodity classifications for encryption computer programs, the first chapter of his textbook, and other items of interest to him. *Id.* The government required a license to export all but one of Junger's programs. *Id.* The government did not, however, require a license to export the first chapter of the textbook. *Id.*

[401] *Junger*, 8 F. Supp. 2d at 711.

[402] *Id.* at 713.

[403] *Id.* at 713-14. Junger's web site also included documents prepared for this litigation. *Id.* at 714. His web site can be found at <http://samsara.LAW.CWRU.Edu/comp_law/jvd/>.

[404] Junger, 8 F. Supp. 2d at 711.

[405] *Id.*

[406] *Id.* The essence of Junger's claim resulted from a strict interpretation of the provisions regarding what exactly constituted an export. *Id.* The Export Regulations control the "export" of specified software. *See supra* notes 83-87 and accompanying text. "Export" of encryption source code is defined by the Export Regulations as "downloading, or causing the downloading of, such software to locations . . . outside the United States . . . unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States." 15 C.F.R. § 734.2(b)(9) (1998); *see supra* notes 83-87 and accompanying text. Junger sought to post encryption programs on his web site. *Junger*, 8 F. Supp. 2d at 714. As a classified "export," such posting required a license. *See* 15 C.F.R. § 734.2(b)(9). Ex-

The court first determined whether the export of encryption software source code was expressive speech protected by the First Amendment.[407] Concluding that the source code was not constitutionally protected, the court stated: "[A]lthough encryption source code may occasionally be expressive, its export is not protected conduct under the First Amendment."[408] The court reasoned that encryption software is inherently functional[409] as opposed to expressive.[410] Emphasizing that the source code does not simply explain a cryptographic process, the court found that the software "carries out the function of encryption."[411] Finally, the court pointed out that where encryption source code is exported, a majority of the time the transfer is for non-communicative purposes.[412] "For the broad majority of persons receiving such source code, the value comes from the function the source code does."[413]

Addressing *Bernstein*, *Junger* found the court's reasoning "unsound."[414] The Junger court opined that *Bernstein* erred in finding language was per se protected speech.[415] "'Speech' is not protected simply because we write it in a language. Instead, what determines whether the First Amendment protects something is whether it expresses ideas."[416]

The court further criticized the analysis of functionality in *Bernstein I* as it related to source code.[417] "Unlike instructions, a manual, or a recipe, source code actually performs the function it describes. While

port Classification Number 5D002 covered four out of the five programs Junger had submitted and were therefore subject to the Export Regulations. *Junger*, 8 F. Supp. 2d at 714. See *supra* text accompanying notes 81-82 for a detailed explanation of the Export Classification Numbers.

[407] *Junger*, 8 F. Supp. 2d at 716.

[408] *Id.*

[409] *Id.* The court defined inherently functional software as code utilized to perform tasks with "scant concern for the methods employed or the software language used to control such methods." *Id.*

[410] *Id.* "Like much computer software, encryption source code is inherently functional; it is designed to enable a computer to do a designated task." *Id.*

[411] *Id.* "The software is essential to carry out the function of encryption. In doing this function, the encryption software is indistinguishable from dedicated computer hardware that does encryption." *Id.*

[412] *Id.*

[413] *Junger*, 8 F. Supp. 2d at 716.

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

[415] *Id.*

[416] *Id.* (citing Roth v. United States, 354 U.S. 476, 484 (1957), and Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 762 (1976)).

[417] *Id.* at 717 (noting that the court's classification of source code in *Bernstein I* as "purely functional," 922 F. Supp. at 1435, is inconsistent with its comparison of source code to instructions and manual-type guidebooks).

a recipe provides instructions to a cook, source code is a device, like embedded circuitry in a telephone, that actually does the function of encryption."[418]

Following the discussion of functionality, *Junger* conceded that the conduct of exporting software may occasionally possess communicative characteristics.[419] The court, however, qualified this finding by stating that "merely because conduct is occasionally expressive, does not necessarily extend First Amendment protection to it."[420] Determining whether occasionally expressive conduct is protected by the First Amendment, the court introduced the standards set forth in *Spence v. Washington*,[421] and applied in both *Texas v. Johnson*[422] and *Tinker v. Des Moines Independent Community School District*.[423]

In *Spence*, the Court required that "[a]n intent to convey a particularized message [must be] present, and in the surrounding circumstances the likelihood [must be] great that the message would be understood by those who viewed it."[424] Applying this standard, *Junger* held source code was not sufficiently expressive.[425] Unlike the communication in both *Johnson* and *Tinker*, the expressive nature of encryption source code is not "overwhelmingly apparent."[426] "Because the expressive elements of encryption source code are neither 'unmistakable' nor 'overwhelmingly apparent,' its export is not protected conduct under the First Amendment."[427]

The final argument entertained by the *Junger* court was whether the Export Regulations were facially invalid as an unconstitutional prior restraint on speech.[428] *Junger* recognized that prior restraints are presumptively suspect before the court.[429] In order to be invalidated, the prior restraint "must have a close enough nexus to expression, or to

[418] *Id.*

[419] *Junger*, 8 F. Supp. 2d at 717.

[420] *Id.* The court cited *City of Dallas v. Stanglin*, 490 U.S. 19 (1989), for the proposition that "[i]t is possible to find some kernel of expression in almost every activity—for example, walking down the street or meeting one's friends at the shopping mall—but such a kernel is not sufficient to bring the activity within the protection of the First Amendment." *Id.* at 25.

[421] 418 U.S. 405 (1974).

[422] 491 U.S. 397 (1989). In *Johnson*, the defendant burned an American flag in government protest. *Id.* at 406. Johnson intended that others, and in fact others did, understand his message. *Id.* See *supra* note 170 for additional background and explanation of the *Johnson* case.

[423] 393 U.S. 503 (1969). In *Tinker*, students wore black armbands in effort to express an unmistakable protest against the United States' participation in the Vietnam War. *Id.* at 505-06.

[424] Spence v. Washington, 418 U.S. 405, 410-11 (1974).

[425] Junger v. Daley, 8 F. Supp. 2d 708, 717 (N.D. Ohio 1998).

[426] *Id.*

[427] *Id.* at 717-18.

[428] *Id.* at 718.

[429] *Id.*

conduct commonly associated with expression, to pose a real and substantial threat" of censorship.[430] Furthermore, the court cited *Roulette v. City of Seattle*[431] for the proposition that "[t]he mere fact that regulated conduct possibly can be expressive is not enough to invalidate a law on its face on prior restraint grounds."[432] Applying the *Lakewood* and *Roulette* standards, the *Junger* court concluded that exporting encryption source code was not conduct "commonly associated with expression."[433] Although the code can be exported for non-expressive reasons, it is commonly transferred for the sole purpose of mandating a computer's operation, a non-expressive activity.[434] Typically, software exportation simply is non-expressive.[435] Finally, the court reasoned that the government regulation did not work a facially unconstitutional prior restraint because the regulations were not "directed narrowly and specifically" at the expressive export of encryption source code.[436] Under the Export Regulations, encryption software is not treated differently than any other encryption technology.[437] Such technology remains subject to the licensing scheme.[438] "[T]he Export Regulations allow academic discussion and descriptions of software in print media while restricting the export of software that can actually encrypt data."[439]

In conclusion, the *Junger* court found that the government's regulations did not work a prior restraint on protected expression.[440] First, Junger failed to present a valid facial challenge to the government's licensing scheme.[441] Second, the regulations were not narrowly focused as expressive conduct.[442]

The *Junger* decision has effectively "tipped the judicial scale" in favor of finding encryption export regulations constitutional. As a result of the *Karn*, *Bernstein*, and *Junger* opinions, future courts have a variety of approaches to explore. If courts follow the *Karn* line of

[430] *Id.* (citing City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 759 (1988)).

[431] 97 F.3d 300 (9th Cir. 1996). In *Roulette*, an ordinance prohibited the act of sitting on the sidewalks to deter expressive acts of activists and street performers. *Id.* at 302. Although sitting on city sidewalks may occasionally be expressive, the law was not found unconstitutional because the conduct is not "integral to, or commonly associated with, expression." *Id.* at 304.

[432] *Junger*, 8 F. Supp. 2d at 718 (citing *Roulette*, 97 F.3d at 303).

[433] *Id.* (quoting *Lakewood*, 486 U.S. at 759).

[434] *Id.*

[435] *Id.*

[436] *Id.* (citing *Lakewood*, 486 U.S. at 760).

[437] 15 C.F.R. § 742.15 (1998).

[438] *Id.*

[439] *Junger*, 8 F. Supp. 2d at 718-19.

[440] *Id.*

[441] *Id.*

[442] *Id.*

reasoning, they will agree that exporting encryption software is expressive conduct subject to the *O'Brien* test of intermediate scrutiny.[443] Under the this test, the courts must find that the government satisfied the four requirements. As argued above, the government has the authority to regulate exports, the regulation clearly furthers important and substantial governmental interests of national security,[444] the government's purpose remains unrelated to regulating free speech,[445] and the regulation is no greater than necessary to further the national security concern.[446]

A second option, the *Junger* line of reasoning, requires a judicial finding that exporting encryption source code is not protected conduct under the First Amendment.[447] The source code may be occasionally expressive, but has an inherently functional quality.[448] Furthermore, the court must find that the government Export Regulations fail to work a prior restraint on expressive conduct.[449]

The *Karn* and *Junger* holdings facilitate government prevention of uncontrollable strong cryptographic technology while maintaining domestic and international demands for effective cryptography.[450] Applying the *Bernstein* line of reasoning is not a highly recommended option, however. "Judge Patel's decision amounted to summary execution of controls on the proliferation of strong crypto."[451] National security is a serious and very real concern of the United States government.[452] Simply dismissing with slight of hand the government's interest in controlling the proliferation of harmful material for the right to speak cryptographically would put national security severally at risk. A computer scientist from Georgetown University warns that immu-

[443] *See supra* Part IV.A.

[444] *See supra* Part II.C.

[445] *See supra* Part V.C.

[446] *See supra* Part V.

[447] *Junger*, 8 F. Supp. 2d at 718; *see supra* notes 406-42 and accompanying text.

[448] *Junger*, 8 F. Supp. 2d at 716; *see supra* notes 408-13 and accompanying text.

[449] *Junger*, 8 F. Supp. 2d at 719; *see supra* notes 428-42 and accompanying text.

[450] "[E]xport controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives intended to preserve U.S. law-enforcement and signals-intelligence capabilities." Stender, *supra* note 2, at 326 (citing U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 9-10 (1994)).

[451] Stender, *supra* note 2, at 315.

[452] *See FBI Says Senate Encryption Bill Could Jeopardize National Security*, COMM. TODAY, July 26, 1996, *available in* LEXIS, News Library, Comtdy File; *see also* Judy Fahys, *Cryptic Coding: Export Quarrel Touches Utah Coding: Conflict about Sales and Spies*, SALT LAKE TRIB., Jan. 28, 1996, at F2 ("The proliferation of encryption of technology threatens the ability of law enforcement and national security officials to protect the nation's citizens against terrorists, as well as organized criminals, drug traffickers and other violent criminals.") (quoting James Cavanaugh, National Security Agency's Deputy Director of Public Policy).

nization from lawful interception is a dangerous road to follow: "We would have havoc in the United States . . . . Lawlessness would prevail."[453]

One additional point needs to be made regarding the balancing of harms. A mistaken ruling in favor of the government would curtail the plaintiff's First Amendment rights. A mistaken judgment against the government, however, could open the flood gates to illegal activity and uncontrollable danger to citizens such as those victims of the Oklahoma bombing and the World Trade Center.[454] Furthermore, software developers have other means of sharing their encryption codes with foreign nations. As the district court in *United States v. Progressive, Inc.* found,

> Because of this "disparity of risk," because the government has met its heavy burden of showing justification for the imposition of a prior restraint, and because the court is unconvinced that suppression . . . would in any plausible fashion impede the defendants in their laudable crusade to stimulate public knowledge of the nuclear armament and bring about enlightened debate on national policy questions, the court finds that the objected-to portions of the article fall within the narrow area recognized by the Court in *Near v. Minnesota*.[455]

B. *Political Impact*

As the courts review and decide encryption software cases, the controversy flows through Congress in attempt to sever the governmental impasse. According to Marcia Smith of the Science Policy Research Division of the Congressional Research Service, "the controversy is over what access the government should have to encrypted stored computer data or electronic communications (voice and data, wired and wireless) for law enforcement purposes."[456] A hearty section of Congressional members strongly promote relaxing export regulations. With equal force, the National Security Agency and the Federal Bureau of Investigation vigorously attack relaxation proposals.[457] If and when *Karn*, *Bernstein*, and *Junger* are appealed to the Supreme Court, the Court's decision regarding First Amendment protection of

[453] Dorothy Denning, *The Clipper Chip Will Block Crime*, NEWSDAY, Feb. 22, 1994, at 35.

[454] The government claims bombing attacks can be intercepted and prevented through the use of key recovery systems. Smith, *supra* note 2, at 13.

[455] United States v. Progressive, Inc., 467 F. Supp. 990, 996 (W.D. Wis. 1979).

[456] Smith, *supra* note 2, at Summary.

[457] *See Does Constitution Protect*, *supra* note 268, at 6D (quoting Barry Steinhardt, President of the Electronic Frontier Foundation and sponsor of the *Bernstein* trial).

software will dramatically affect the factors considered throughout the Congressional debate.[458]

Many proposed bills that argue for relaxation of encryption export controls are presently before Congress. These proposals are more concerned with monetary gain or international trade,[459] as opposed to the judiciaries' constitutional concerns.[460] Three pieces of legislation before the 105th Congress challenge the government's export regulations on encryption technology.[461]

Senator Conrad Burns of Montana introduced the Pro-CODE[462] Act of 1997 bill, which basically proposes an elimination of export controls on encryption technology.[463] The bill prohibits mandatory key recovery and liberalizes export controls by requiring reports submitted to the Secretary of Congress after the product has already been exported as opposed to a condition of obtaining a license.[464] Clearly, the intent of the bill is to eliminate export control of encryption technology.

A second proposed bill relating to the export of encryption technology is Senator Patrick Leahy's Encrypted Communications Privacy Act of 1997 ("ECPA").[465] The ECPA is similar to Burns' Pro-CODE in that it targets export regulations. The ECPA varies in numerous ways. First, if a key recovery system was used, the ECPA would per-

[458] One opponent of strict governmental regulations predicts a commercial impact and societal use impact:

> At stake in the broad debate over the export of encryption software is the use of encryption by U.S. citizens at home. Legal experts say that as long as domestic manufacturers are prevented from exporting strong encryption products abroad, they will not manufacture and distribute those same wares in the United States, where the use of encryption is legal.

Does Constitution Protect, *supra* note 268, at 6D (quoting Barry Steinhardt). If finding software protected speech results in complete decontrol of exporting encryption technology, law enforcement and national security intelligence members strongly suggest that criminals, terrorists, and foreign intelligence targets of interest would eventually disappear and move completely undetected. *See* Hoffman, *supra* note 102, at 549. In effect, Congress would severely handicap the government's ability to maintain and protect security of the United States and its citizens. *Id.*

[459] *See* Smith, *supra* note 2, at 8-10; *Showdown on Encryption*, *supra* note 233, at C6.

[460] The government's response to any attempt to weaken export controls on encryption software, however, is one of a national security concern. *See supra* Part II.C.

[461] *See* Smith, *supra* note 2, at 8-10.

[462] Pro-CODE essentially stands for: "The Promotion of Commerce On-line in the Digital Era Act." S. 377, 105th Cong. (1997).

[463] *See* S. 377. For a summary of the bill's specific elements, see Smith, *supra* note 2, at 10, or *Bill Summary and Status Information*, Digest, § 377 (visited Nov. 30, 1998) <http://thomas.loc.gov/cgibin/bdquery/z?d105:SN00377:@@@L>.

[464] S. 377.

[465] S. 376, 105th Cong. (1997). For a summary of the specifics of the bill, see Smith, *supra* note 2, at 9-10.

mit law enforcement access to keys under court order.[466] Second, any United States individual may use encryption in any state or foreign country, regardless of the software's strength.[467] Third, ECPA would criminalize using encryption products to obstruct justice.[468] Finally, the ECPA would protect as well as penalize "key holders."[469]

A third bill addressing the export of encryption technology is known as the Security and Freedom Through Encryption Act ("SAFE"). Introduced by Representative Bob Goodlatte of Virginia, SAFE also reduces export controls on encryption products.[470] Specifically, the bill relaxes controls on products available through international markets.[471] Similar to the other proposed bills, SAFE prohibits mandatory use of key recovery, permits free use of any strength encryption produce, and creates criminal sanctions for using encryption to obstruct justice.[472]

The above mentioned bills advocate relaxing export controls on encryption products. Senator Leahy stated, "[t]hese bills . . . roll back current restrictions on the export of strong cryptography so that high-tech U.S. firms are free to compete in the global marketplace and meet the demands of customers—both foreign and domestic—for strong encryption."[473] The future success of any of these proposals is difficult to predict. Apparently, the congressional and constitutional challenges present a trend in relaxing export controls without complete decontrol.

VII. Conclusion

Cryptography is an essential tool for ensuring secured communications. Unfortunately, such technology is occasionally utilized to privatize messages intended to harm or (worse yet) destroy individuals, society, the government, or any other targeted victim. Controlling the proliferation of cryptography enables the government to intercept, decipher, and potentially trace a message back to a potential terrorist, drug trafficker, or other felonious agents before the victim is harmed.

[466] S. 376, § 2802.

[467] *Id.* § 2805.

[468] *Id.* § 2804.

[469] *Id.* § 2802; *see supra* notes 54-58 and accompanying text (explaining the key recovery mechanism).

[470] H.R. 695, 105th Cong. (1997). For a summary of the bill's specific elements, see Smith, *supra* note 2, at 8-9.

[471] H.R. 695, § 2803.

[472] *Id.* §§ 2803-05.

[473] *Encryption Bills Make Their Way Back to Capitol Hill*, Comm. Today, Feb. 28, 1997, *available in* LEXIS, News Library, Comtdy File.

In efforts to control cryptography, the government placed regulations on the export of cryptographic software on computer disks. These regulations have been challenged as an unconstitutional violation of the First Amendment.

Plaintiffs Bernstein, Karn, and Junger constitutionally challenged the United States government's regulation of encryption technology. They essentially argued that the government licensing scheme shackles their First Amendment right to speak freely. The *Bernstein* court found the government regulations worked a prior restraint on protected speech. The *Karn* court similarly held that software is speech protected under the First Amendment. Most recently, the *Junger* court found, *inter alia*, that the government's export regulations were constitutional. The court concluded that the regulations were not directed at expressive speech.

The government does not deny companies and the general public's justifiable demand for utilizing strong encryption. The First Amendment, however, should not function as a vehicle to completely divest the government's imperative control in this area. "First Amendment protections for pure speech are justifiably far-reaching; however, crypto is hard pressed to fall within those protections because it lacks the expression needed to invoke those protections."[474]

Yvonne C. Ocrant

[474] Stender, *supra* note 2, at 317.