2 Va. J.L. & Tech. 3 (Fall 1997) <http://vjolt.student.virginia.edu>
1522-1687 / © 1997 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL *of* LAW *and* TECHNOLOGY

| UNIVERSITY OF VIRGINIA | FALL 1997 | 2 VA. J.L. & TECH. 3 |
|---|---|---|

# Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security

## by E. John Park[*]

# I. Introduction

1. Communication related to technological information -- data, know-how, and software source codes -- is increasingly important in today's society. At the same time, scientific speech presents a problem for First Amendment analysis because it is unclear whether the free expression of scientific ideas and techniques enjoys the same protection accorded political speech. As science and technology provide new kinds of products and more controversial uses, the delicate balance between protecting individual expression and governmental interests in controlling the free flow of technology-related information becomes more difficult to preserve. Clearly, scientific communication can be limited when necessary to directly address national security interests and in cases where such communication results in the transmission of dangerous technologies to governments or criminals.
2. The question many courts and policymakers currently confront is how strictly or severely regulatory controls can limit the free flow of scientific information. In other words, do export controls and additional government classifications of new technological products based on these controls or government standardization of such technologies collectively negate free speech related to the computer software field and impinge upon core First Amendment values? Oliver Wendell Holmes, in his dissent in *Abrams v. United States*, coined the "marketplace of ideas" metaphor in explaining a fundamental rationale for free speech protection: "...the ultimate good desired is better reached by free trade in ideas - that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution."[1] Another rationale for granting free speech is that an individual's personal autonomy must be guarded in order to preserve free expression. In an age of new technologies and ideas, each of these rationales suggests that increased government controls may impermissibly limit the free competition of ideas and suppress independent expression.
3. Recently, debate over the question of increased government controls has focused on the distribution of new technologies that allow its users to mask their identity when fusing electronic mail or "e-mail" and to encrypt or cypher electronic communications. Encryption software[2] enables on-line users to protect the confidentiality of information sent over the Internet. Specifically, encryption source codes, or the programming text that drives the software, are based on advances in cryptography - the science of writing programs that distinguish messages, using codes and ciphers so that selected people can interpret the message.[3] This software is used in various forms of electronic communication, most notably communication that involves commercial transactions**.** The financial services industry, for instance, employs encryption to protect the confidentiality of fund transfers totaling more than two trillion dollars on a daily basis.[4] In addition, encryption source codes are used by computer system operators to protect the confidentiality of passwords and by individuals to protect the privacy of electronic mail sent over the Internet.[5]
4. Encryption source codes, as the programming text for software, represent a form of speech and, thus, merit a degree of free speech protection from export controls and government-mandated requirements. Nonetheless, the National Security Administration (NSA) and others in the

intelligence community have raised national security concerns in connection with source code distribution that may render communications related to illegal activity un-monitorable. In addressing these concerns, the NSA has strictly enforced export restrictions on encryption source code distribution and has promoted the use of government designed encryption source code as an industry standard.

5. These policies have prompted much criticism and activity on the part of free speech advocates, the Electronic Frontier Foundation (EFF) and individual litigants. Two recent cases, *Bernstein v. U.S. Department of State*[6] and *Karn v. U.S. Department of State*[7] are the first to address First Amendment arguments that NSA controls unduly restrict free speech. In *Bernstein*, the United States District Court for the Northern District of California granted injunctive relief from NSA export controls and found that such controls impermissably limit free speech.[8] In *Karn*, the United States District Court for the District of Columbia, in contrast, found that NSA export controls do not unduly suppress free speech.[9] On the legislative front, at least three bills are pending in Congress that would change federal encryption policy.[10]
6. In summary, the current debate revolves around two competing interests: free speech advocates and software industry representatives support free encryption source code development and distribution, while the NSA restricts exports of such codes as menacing paraphernalia and promotes the use of standardized encryption source code which can be more easily deciphered by government agencies.
7. These competing interests raise a number of doctrinal issues. The following paper focuses on whether current controls may violate First Amendment protection of scientific speech. The transmission of encryption source codes over the Internet represents a form of scientific speech because the information that software developers seek to transmit represents the results of research and advances in cryptography. As such, it is the communication of encryption techniques rather than the communication that encryption masks that is at issue.
8. As the line between speech and machine or technological ideas becomes more obscure, current restrictions in the name of national security may undermine core First Amendment values and scientific expression in that software developers will be unable to freely promote and discuss their most recent programs and innovations. Section I reviews the evolution of NSA policies that restrict exports of so-called dangerous technologies, focusing on encryption source codes and presenting the doctrinal issues these regulations raise. The doctrinal difficulties of First Amendment analysis in this area relate to whether current restrictions are labeled as content-based as opposed to content-neutral. The *Karn* and *Bernstein* decisions arrive at different conclusions regarding this question. The *Karn* court applied content neutral standards of review, while the *Bernstein* court applied content-based standards of review. Section II compares and contrasts the *Karn* and *Bernstein* approaches. Given that previous decisions have led to inconsistent results, Section III argues that the *Karn* approach may be under protective of speech and suggests a theory of protection in line with the reasoning in *Bernstein* that takes into account core First Amendment values such as the marketplace of ideas as well as personal autonomy as rationales for protecting scientific expression.

## II. Background and Doctrinal Issues

### A. Encryption Technology

9. Encryption software protects electronic communications from the misuse of others and is designed to address the information security problems of a range of users from individuals to large financial institutions to government agencies. It provides a secure method of communicating where interventions by malfeasants are increasingly possible because computer systems allow for multiple access points by such users.
10. Specifically, encryption software is used to authorize transactions, authenticate users, verify the accuracy of messages and documents, certify legitimate transactions, as well as protect individual privacy. These applications make possible computer-based finance and commerce such as Internet transactions and automated teller disbursements. The source code that drives the software is based upon various techniques or mathematical algorithms for encrypting messages and information. Each algorithm uses a series of numbers known as a key that can be altered with each message or user according to a fixed schedule. Generally, this combination of numbers resemble, in more complex form, a locker combination or other forms of personal identification numbers. As such, keys are selected so that they cannot be easily deciphered and are made as random as possible. In this way, an adversarial user cannot determine a pattern linking a series of keys based on a single key's algorithm.
11. These advantages, however, in the hands of foreign governments or criminals may make it difficult for the NSA to gather information and monitor communication related to illegal activity. Unbreakable forms of cryptography for personal use, thus, could frustrate the execution of justice and threaten public safety. For instance, in a recent California case, authorities arrested an individual for sending child pornography via e-mail.[11] Officials were unable, nonetheless, to seize critical evidence because a significant amount of the communications had been ciphered through encryption software. As such, NSA regulations are designed to standardize encryption software used within the United States and to stem the flow of source code techniques to users abroad.

### B. National Security Restrictions on Encryption Technology

12. The NSA has adopted two policy approaches designed to confine the flow of encryption software. First, the NSA has strictly enforced export controls[12] on distribution over the Internet. Export controls are a form of legislated restraint on scientific communication. They are primarily the result of Cold War security imperatives and designed to address limited access to military source code. With the advent of the Cold War, the U.S. government imposed export controls to prevent the Soviet Union and the Warsaw Pact nations from accessing U.S. technology that could enhance the military capabilities of the Communist block. As such, Congress enacted the Export Administration Act in 1979.[13]

#### 1. The Export Administration Act

13. The Act was in part a response to a Defense Science Board panel directed by Fred Bucy that emphasized the need for secrecy in scientific research. The Bucy panel found that knowledge

requiring restrictions was not limited to military equipment but also included design and manufacturing know-how. As a result, the Bucy panel advocated the expansion of the term "military useful" to include design concepts and manufacturing processes. The Act, as such, reflects an effort on the part of Congress to control the export of scientific concepts and technological ideas.[14] The Act controls the export of "goods and technology which would make a significant contribution to the military potential of . . . countries which would prove detrimental to national security."[15] Technology is defined to include "information and know-how (whether in tangible form . . . or intangible form) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data."[16]

14. Under these provisions, the Department of Commerce promulgated the Export Administrative Regulations.[17] The Act also formally authorized United States participation in the Coordinating Committee on Multilateral Export Controls with sixteen other allied nations.[18] Known as COCOM, this informal multilateral export control body was designed to develop uniform policies among all the affiliated nations. Although COCOM was formed in order to develop uniform export standards, currently the COCOM countries and other U.S. trading partners have adopted a range of approaches.
15. The NSA in coordination with the Bureau of Export Administration (BXA) administers controls over products that cover a range of industries that export source code and software. Generally, for software exports a special license known as a "General License GTDR" is granted with few restrictions to exporters of software that is generally available to the public. Such software must be sold from stock at retail selling points, without restriction, by means of: 1) Over the counter transactions; 2) Mail order transactions; or 3) Telephone call transactions.

### 2. The Commodity Jurisdiction Application Process

16. In 1988, the United States initiated export controls of encryption source code specifically with the passage of the Arms Export Control Act (AECA).[19] It regulates the exports of "defense articles" and "defense services" in order to promote "world peace and the security and foreign policy of the United States."[20]As such, under the AECA Congress authorized the President to compile a list of "defense articles" that are restricted from export. The State Department includes 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 as defense articles. This enforcement has restricted distribution of dangerous technologies in order to insure that encryption programs are not made available to governments and criminals abroad.[21] Under ITAR, the State Department's Office of Defense Trade Controls (ODTC) has primary jurisdiction over encryption source codes.[22] Export of defense articles such as cryptographic source codes are administered by the NSA under ITAR.[23]
17. The NSA determines whether an item is a defense article through the Commodity Jurisdiction application process. Under this process, software developers are required to seek State Department approval prior to transmitting encryption source code and software over the Internet. Once an application is received, the NSA systematically checks for ITAR applicability.[24]

Currently, under ITAR, the NSA has precluded the export of any encryption source codes of greater than 40 bits.[25] The diluted encryption levels allowable for export affects most algorithms available in the market today and only permits the export of the weakest forms of encryption source code.

18. Second, the NSA has promoted the use of key escrow source code which is popularly known as the "Clipper Chip"[26] in order to allow the government access to keys that can decrypt communications or computer stored information.[27] In 1994, the NSA implemented the Clipper Chip program through enforcement of its Escrowed Encryption Standard (EES).[28] The key escrow source code encryption scheme involves the storage of private source code keys with the NSA to allow for the decrypting of encoded messages when deemed legally necessary.[29] Those utilizing key escrow source code would automatically have half of the private key they use to encrypt to their messages recorded and sent to government "storage banks," while retaining the other half of the private key.[30] Should a court grant the government the right to access both halves of the key, the government would be able to decrypt any message sent. The NSA anticipates that by creating such a encryption technique, it will facilitate the use of EES by businesses and individuals, thereby giving the government the ability to decrypt their messages or computer stored information when necessary.

### C. The Doctrinal Dilemma: Content-Based v. Content-Neutral Standards of Review

19. These regulations may collectively suppress scientific expression, and the Commodity Jurisdiction application process may impose an unconstitutional prior restraint on speech. Source codes or the programming text that drive encryption software are akin to scientific expression and academic literature and thus represent a form of speech. Full protection is generally accorded scientific results or theories that are published. Early decisions regarding scientific speech that contained obscene elements provided the Supreme Court with its first opportunity to address the constitutional status of scientific speech. In *Roth v. United States*, the Court held that science was safely outside the category of obscenity and should be accorded full protection.[31] In *Miller v. California*, the Court held that the "First Amendment protects works which, taken as a whole, have serious...scientific value."[32] Similarly, in *F.C.C. v. Pacifica Foundation*, the plurality specifically retained a high status for scientific speech.[33]
20. Restraints on speech, nonetheless, are permissible if the restrictions, among other things, further a substantial governmental interest.[34] The questions many courts will face in the future as software developers seek to distribute more security-sensitive source codes and programs over the Internet is how substantial the government's national security interests are in restricting the distribution of technological advances and scientific speech. Existing First Amendment doctrines provide a number of standards for evaluating the government's national security justifications, though it is unclear which standard ought to be applied in evaluating restrictions on scientific expression over the Internet.
21. Content-based restrictions control speech on the basis of the subject matter of the speech such as dangerous or security-sensitive information like encryption technology. Content-neutral restrictions limit speech on the basis of the channel of communication such as transmission over

the Internet rather than content. Consequently, restrictions on software developers attempting to use the Internet to reach their counterparts abroad in order to receive feedback regarding encryption source codes or to transmit encryption source codes to users abroad may be tested as either content-based or content-neutral regulations. Because the standard of review for content-based restrictions demands higher scrutiny as opposed to content-neutral restrictions, whether NSA regulations are permissible depends in large part upon how courts categorize current policies. The following discussion compares the analysis in the *Karn* and *Bernstein* decisions, and then argues that the *Karn* approach is under protective of protective in view of core First Amendment values.

## III. Analysis

### A. Export Controls as Content-Neutral Restrictions

22. In *Karn* the United States District Court for the District of Columbia found that the AECA and the ITAR licensing schemes are content-neutral regulations and applied the deferential *O'Brien* standard of review.[35] Philip Karn, a software developer who designed several encryption source codes, submitted two commodity jurisdiction applications to the NSA: one to publish a book containing the source and a second to distribute the software source code over the Internet in order to receive feedback from cryptography experts abroad.[36]
23. The NSA approved the application for the book and found that the source code in print form was not a defense article. Nonetheless, the NSA denied the application for Internet distribution of the exact same source code in software form.[37] Karn sought injunctive relief from NSA enforcement under ITAR, and the court found that the licensing scheme was a content-neutral restriction, that the NSA retains a substantial interest in regulating exports of source code, and that current restrictions are not overbroad.[38] Karn did not dispute the government's argument as to the first two prongs of the *O'Brien* test (related to governmental powers and interests).[39] Karn did attempt to challenge the government's claim that NSA enforcement of ITAR met the second two prongs (related to suppression of free speech and overbreadth) and attempted to argue that, given that encryption source code is already widely available in other countries, the NSA's restrictions go farther than is necessary to further national security interests.[40]
24. The *Karn* court declined to accept this argument and deferred to the government's position that enforcement of ITAR is not overbroad.[41] In fact, the *Karn* opinion avoided questioning the NSA's policy judgment on this issue.[42] The court disposed of these arguments by finding that the NSA's enforcement of ITAR and AECA did not violate the First Amendment and that under the political question doctrine policy issues related to encryption policy and national security were beyond the "extremely limited scope" of judicial inquiry.[43]
25. In *Karn*, the court was persuaded by the government's argument and by the Ninth Circuit's interpretation of ITAR in *United States v. Elder Industries*, holding that export controls are not overbroad and do not suppress free speech.[44]
26. The *Karn* court's reluctance to question the national security justifications for encryption source

code restrictions reflects the difficulties of First Amendment analysis in the national security context. As new technologies present additional opportunities for government classifications of dangerous ideas and thus more restrictive policies, core First Amendment values and scientific expression may be negated. Without doubt, courts do not have the expertise or mandate to evaluate controversial policy issues related to national security that are best addressed by the political branches of government. In *Baker* v. *Carr*, the Supreme Court made clear that it would not interfere with such political considerations.[45] More recently, in *United States v. Martinez*, the United States Court of Appeals for the Eleventh Circuit found that national security determinations "possess nearly every trait that the Supreme Court has enumerated traditionally renders a question political."[46]

### B. Export Controls as Content-Based Restrictions

27. In *Bernstein v. United States Department of State*, the United States District Court for the Northern District of California found that, in contrast, export controls are content-based restrictions and thus demand strict scrutiny.[47] Daniel J. Bernstein, a mathematics graduate student at the University of California, Berkeley, wrote an encryption source code known as "Snuffle" which he planned to distribute over the Internet.[48] Since export products related to source code are considered "defense articles" by the NSA under the AECA and ITAR, Bernstein, like Karn, was required to submit a Commodity Jurisdiction request with the NSA as a precondition to applying to export Snuffle over the Internet as required by ITAR.[49]
28. Under ITAR, the NSA conducted the Commodity Procedure evaluation in order to make the determination of whether a product is considered a "defense article."[50] In August, 1992, the NSA informed Bernstein that Snuffle would be considered a defense article under Category XIII of the ITAR and was prohibited from export.[51]
29. Bernstein, consequently, sought injunctive relief from NSA enforcement of AECA and ITAR on the grounds that both the acts and the regulations restrict protected speech, arguing that licensing requirements under ITAR create an unconstitutional prior restraint on speech.[52] The government moved to dismiss on the ground that the claim was precluded by the ITAR legislation and that the source code for the encryption program was not speech but conduct covered by ITAR because source codes, as a functioning cryptographic product, do not convey or express a particular message. As such, source code would not be speech in that its purpose is functional rather than communicative.[53]
30. In allowing Bernstein to proceed with his suit and denying the motion to dismiss, the *Bernstein* court found that the Snuffle encryption source code, though containing potentially dangerous technology, was "speech of the most protected kind."[54] Consequently, the *Bernstein* court rejected the argument that conduct must be sufficiently imbued with elements of communication to be symbolic speech and found that source codes fall within the protection of the First Amendment.[55]
31. Under content-based analysis, the *Bernstein* court also found there is a "heavy presumption" against the constitutional validity of such a restriction on speech.[56] National security

considerations throughout history have at times warranted prior restraints based on classifications of technology as threats to national security. Although courts have not precisely defined the limits of such classifications of information that represent a prior restraint on speech, generally content-based restrictions on the distribution of technological information are impermissible. The leading decision in this content-based restrictions area is *Near v. Minnesota*.[57] In *Near*, the Supreme Court held that, with certain limited exceptions, prior restraints on the dissemination of scientific information are constitutionally impermissible.[58]

### C. Analytical Comparisons

32. If courts apply the content-neutral standard, then they may not give weight to the value of scientific freedom or examine critically the nature and magnitude of the threatened harm to national security.[59] Alternatively, if courts apply the content-based standard, they will be forced to address political questions regarding national security interests and make value judgments regarding the benefits of scientific expression. The *Karn* court opted to apply the content-neutral standard and under the political questions doctrine declined to parse the NSA's national security justifications.[60] The *Bernstein* court's analysis applied the content-based standard, questioning the government's national security concerns justifications and concluding that current restrictions are overbroad.[61]
33. For the most part, the debate about restrictions on new technologies has centered on threats to national security and on whether political questions are beyond the scope of judicial analysis. In *Bernstein* and *Karn*, the legal analysis necessarily addresses the NSA's position in relation to statutory language provided in export control legislation. Nonetheless, limiting scientific expression may not always be equated with national security, and the *Karn* content-neutral analysis may not adequately protect free speech.
34. Content-neutral analysis and the political questions doctrine prevent courts from parsing arguments based on national security justifications. Nonetheless, export restrictions that limit communications regarding technological information can be distinguished from political questions that trump judicial review because a good faith free speech challenge must be fully addressed by the courts. As to free speech issues, courts possess the required expertise to adjudicate these issues and should not allow embedded policy questions to prevent them from interpreting rights that ought to be addressed or making value judgments that scientific speech as a social good merits protection. As noted by the Supreme Court in *Baker*, "The doctrine . . . is one of 'political questions' not one of 'political cases,'"[62] and courts should not shy from controversies where state action labeled as "political" limits free speech.
35. The *Bernstein* content-based analysis, in contrast, permits courts to focus on whether the government's national security concerns may justify restrictions on scientific speech. If courts were to strike down restrictions generally as an impermissable restraint on speech, however, they would inevitably be making value judgments related to the social value of scientific speech. Specific threats to national security may constitute a substantial interest that makes it necessary to limit free speech. In *Schenck v. United States*, the Supreme Court found that an impingement on free speech in certain circumstances appears to be a reasonable exercise of sovereign power in the

interest of the common defense and security.[63]

## IV. Argument

36. Although the *Karn* and *Bernstein* decisions come to different conclusions regarding the appropriate treatment of export controls as content-neutral or as content-based restrictons and have applied different levels of scrutiny, it can be argued that the ITAR licensing scheme is a content-based regulation. Content-based restrictions control speech based on the dangerous ideas that the regulations seek to confine.
37. The commodity jurisdiction procedure under the ITAR statute broadly limits the entire cryptography field because of the dangerous nature of the technology in the hands of foreign governments or criminals.[64] The NSA stands upon this statutory language in enforcing current export restrictions.[65] This language may be overly broad in that it permits the NSA to suppress any and all communications about encryption source codes and therefore may be impermissible under the First Amendment. The technical data definition may be overbroad because it does not retain any reasonable degree of constraints on NSA authority.[66] Technical data includes "information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation."[67] This language may prohibit a range of speech. For instance, an expansive reading would even prohibit a lecture or speech regarding encryption source codes where foreign nationals are present.

### A. A Theory of Protection: Parallels to *United States v. Progressive, Inc*.[68]

38. Under a content-based analysis, export controls in encryption software may be viewed as akin to content-based restrictions on the publication of confidential government or security-sensitive information. In this area, the Supreme Court has previously developed a large body of jurisprudence related to constitutional guarantees in the national security context that demand strict scrutiny on the part of courts and support broad protection of speech.[69] Under this line of reasoning, encryption software and cryptography developers can be equated with individuals who have tried to publish confidential government documents or information and have been accorded a high degree of speech protection.
39. Consequently, even if the national security interests warrant some form of prior restraint on the free flow of information, courts must still provide judicial review before content-based restrictions can be imposed. In *Freedman v. Maryland*, the Court set forth procedural protections that must be accommodated before upholding content-based restrictions.[70] A restraint is valid only where the administrator acts within a specified period of time and where prompt judicial review is available to prevent an erroneous denial of a license or permit to proceed.[71]
40. Assuming encryption software parallels the confidential information line of cases, export controls can be directly scrutinized in terms of their policy justifications. In *United States v. Progressive*

*Inc.*, the United States Court of Appeals for the Seventh Circuit dismissed the government's suit against *The Progressive*, a newspaper that was seeking to publish technical information regarding how to construct an atomic bomb, because similar information regarding the construction of atomic bombs had already been published and was freely available.[72] The government had argued that the release of such technical information posed a threat to national security,[73] but the Seventh Circuit, in dismissing the appeal, thought otherwise.

41. Similarly, it is unclear whether NSA enforcement of ITAR in fact serves to protect national security interests. Much of the prohibited source code is already freely available abroad. A study by the Software Publishers Association found that 164 of the high-level encryption source codes that may not be exported under current export controls are already available in foreign markets.[74] Although the NSA has strictly enforced existing rules and regulations such as ITAR in controlling encryption source code exports, Internet distribution from points outside the United States also make it increasingly difficult to confine the dispersion of encryption source code technology notwithstanding controls. For example, a popularly available source code known as Pretty Good Privacy (POP) was released for free on the Internet by graduate students in England.[75] Consequently, a researcher at the Virus Test Center at the University of Hamburg in Germany received a copy and made a copy available on his globally popular Internet distribution site.[76] Other copies were then made available at Internet distribution sites in France and Italy. In effect, NSA enforcement of ITAR may not serve a substantial government interest because no level of export controls can truly resolve national security concerns.[77]

**B. Overbreadth**

42. As such, current NSA restrictions may not be drawn narrowly enough to escape impermissibility under the First Amendment. Under ITAR, exports include "sending or taking a defense article out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data," or "disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[78]
43. Nonetheless, the ITAR definition of technical data was limited by the United States Court of Appeals for the Ninth Circuit in *United States v. Edler Industries, Inc.* to communications where information "significantly and directly related to specific articles on the Munitions List."[79] The *Elder* court narrowed ITAR substantially in order to avoid serious interference with "the interchange of scientific and technological information."[80] Specifically, *Elder* requires the government to know or have reason to know that the information in question is intended for a prohibited use.[81] The court's explicit sensitivity to the important of protecting the free dissemination of scientific knowledge suggests that the statute cannot be applied by the NSA in a manner that overly restricts or impinges upon scientific communications.
44. Moreover, some commentators have concluded that NSA enforcement of ITAR goes beyond what is required in the name of national security and, on balance, free speech concerns outweigh the need for enforcement.[82] Kenneth W. Dam, for instance, has argued, "As for export controls on cryptography, they have . . . helped to deny the benefits of cryptography to foreign

adversaries."[83] Current controls may go beyond what the legislation supports. They may also work to reduce the domestic availability of strong encryption and restrict U.S. sellers of technology from exporting products with such capabilities, even when foreign customers can buy them elsewhere, and in so doing limit exports to a greater extent than necessary.[84]

### C. First Amendment Values: The Importance of Scientific Speech as a Social Good

45. Even at the height of the Cold War, Vannevar Bush recognized that a broad dissemination of scientific information upon which further advances can readily be made furnishes a sounder foundation for our national security than a policy of restriction which would impede our progress in the hope that our possible enemies would not catch up with us."[85] The Supreme Court's free speech jurisprudence in many senses supports such a view. The marketplace of ideas rationale articulated by Justice Holmes and expanded upon by others[86] covers a wide range of expression and was not reserved exclusively for political speech. Although there are no explicit decisions creating a right to scientific inquiry, some have argued that such a right is implicit in the First Amendment.[87]
46. Consequently, this line of reasoning suggests that restrictions that silence software developers or technologists and limit their ability to freely communicate and develop their ideas would threaten communications at the core of the First Amendment. The marketplace rationale as such can more broadly be conceptualized as protecting scientific discourse and research as well as political speech. In this manner, the search for truth is a search for accuracy and efficiency in how science shapes new technologies, in much the same way that the search for truth in the political arena requires the free expression of ideas.
47. In certain instances, courts have elevated scientific speech to the status of core political speech. In *Firestone v. First District Dental Society*, the a New York court found that radio broadcasts of scientific dental matter were akin to political speech.[88] An unfettered marketplace of ideas allows for the ascendancy of the most valid and compelling views and ideas and as such may promote scientific and technological advances. Government standards and restrictions may supplant the free flow of scientific ideas and limit research. The marketplace and the First Amendment under this rationale ought not undermine the process of discovery or distort scientific outcomes. As Vincent Blasi argues, "any governmental intervention in the market is likely to exacerbate rather than ameliorate the preexisting distortions, thereby adding . . . [a] hindrance to the quest for truth."[89]
48. Similarly, the personal autonomy rationale for free speech protection may support open scientific communication. Free speech in the scientific context allows for an individual to select subject matter, means of communication, and sources of critical assessment.[90] These fundamental rights in many senses are also reflected by the First Amendment and the personal autonomy model of free speech. Under this model, an individual, such as the University of California, Berkeley, mathematics graduate student who developed the "Snuffle" encryption source code that was at the center of the *Bernstein* case, acts as "[a]n autonomous agent [that cannot] accept the judgment of others as authoritatively deciding what the agent ought to believe or how the agent should act."[91]

49. Accordingly, current NSA policies limit individuals such as software developers in fully exploiting and exploring their theories and ideas in a manner that may infringe upon free speech. As is the case with the marketplace ideas, the personal autonomy model may be conceptualized to include scientific ideas and theories. Software developers under this model need to be free to develop their ideas and to test their accuracy. The content of these ideas cannot be confined under government standards or controls as irrational or dangerous, because this thwarts individual expression. Martin Redish notes that "[a]n individual's 'mental' processes cannot be limited to the receipt and digestion of cold, hard theories and facts, for there is also an emotional element that is uniquely human and that can be 'developed' by . . . non-rational . . . communication[s]."[92]

50. The core values represented by both the marketplace and autonomy models may support more flexible standards for testing the constitutionality of the NSA's policies. The difficulties in applying the appropriate standard of review as reflected by the contradictory *Bernstein* and *Karn* opinions suggest that pre-existing doctrines do not fully address the free speech issues associated with new technologies and forms of expression. Consequently, alternative modes of analysis that consider the social values related to scientific speech may in the future provide more direction for courts.

### D. An Alternative Framework

51. An alternative analytical framework may provide some guidance for courts in the future.[93] Based upon the Court's analysis in the commercial speech area,[94] the First Amendment can be viewed as supporting a general societal interest in the free flow of information that may allow courts to justify striking down government controls in the future. The framework would focus on three interests related to scientific speech: (1) an individual interest in the self-expression of scientific ideas, (2) a general interest in the free flow of scientific information, and (3) a societal interest in technological advancement.

52. These interests recognize that the First Amendment was originally drafted in part to further progress in science and technology and that the Framers viewed scientific speech as worthy of protection as political speech. Thomas Jefferson, for example, strongly opposed tariffs on scientific treatises and argued that "science is more important in a republican than in any other government."[95]

#### 1. Compelled Speech

53. In light of these interests, the NSA requirement of disclosure of encryption keys can be viewed as compelled speech, similar to financial disclosure requirements for publicly traded companies. In the noncommercial context, the Supreme Court views mandatory disclosure requirements as content-based restrictions on free speech. In *Riley v. National Federation of the Blind*, the Court found that "[m]andating speech that a speaker would not otherwise make necessarily alters the content of the speech."[96] Under *Riley*, noncommercial mandated disclosures are permissible if they serve a compelling state interest, avoid undue burdens on free speech, and are narrowly tailored.[97]

54. For example, in *Wooley v. Maynard*, the Court struck down a New Hampshire statute mandating cars to carry license plates displaying the state motto, "Live Free or Die," because the policy in question did not serve a compelling state interest.[98] In the encryption source code context, national security and law enforcement concerns are well established compelling state interests. As such, the question is whether burdens created by forced disclosure of encryption keys are necessary to serve national security interests and whether they are narrowly tailored. Specifically, mandatory disclosure requirements are permissible if there "is a 'relevant correlation' or 'substantial relation' between the governmental interest and the information required to be disclosed."[99]

55. The NSA has stated that implementations which are tested and validated by NIST will be considered as complying with that standard.[100] While the EES mandate that the use of the Clipper Chip to be restricted to with government-specified algorithms and appears to narrowly tailored, it does not specify what types of government equipment purchases are covered.[101] As such, EES represents a type of rule where by standards have binding effect without announcing to the public how the NSA will act in the future, or how the NSA will assess the impact of the rule.[102] EES's imprecision makes it possible that the regulations in effect may apply to a broader pool of users and impinges upon progress in computer software science generally. It is likely that software developers will adopt the Clipper Chip as standard encryption equipment, because EES does not make clear the range of products that are covered. EES also preempts the development of software and scientific advancements which are moving the encryption techniques toward software applications. Some commentators have suggested that EES may be overbroad in effect and does not take into account individual choices of software developers.[103]

56. EES represents the federal government's strategy to employ its market power to create a national encryption source code standard, whereby no congressional appropriations are involved, taking Congress out of the decision-making process.[104] The government often creates "non-legislative rules" by setting government purchasing standards under the FIPS that apply to the broader market. EES, however, creates industry standards which may affect the free speech rights of software developers in a manner that limits accountability and congressional oversight. Moreover, standards for government equipment have a significant impact on technology industries where a substantial segment of the market is driven by government purchasing preferences. For example, the day the NSA introduced the Clipper Chip program and EES, AT&T announced that all of its new telephone and computer production lines would be equipped with the Clipper Chip.[105] Also, it is unclear whether EES, from an implementation point of view, will fully serve the NSA's intelligence gathering objectives. EES will not prevent those who are most likely to conduct illegal communications or transactions from employing encryption systems that are free of government standards. The NSA notes "that it has chosen to encourage the widespread use of key escrow source code devices to make encryption technology more controllable and allow for government monitoring."[106] However, even if the government hopes to monitor on a regular basis, as indicated in this statement, it remains unclear whether criminals whose exact communications the government seeks to monitor will use government encryption software. Additionally, it would be possible for those using the Clipper Chip for illicit purposes to encrypt their information one stage before the Clipper encryption, thereby still frustrating the objectives of

law enforcement.[107] Consequently, the limited effectiveness of the Clipper Chip program suggests that EES places a burden on speech and individual software developer freedoms that are not worth the supposed gain to national security and that there is no "relevant correlation" between EES and security objectives.

57. Moreover, government standardization of encryption techniques may undermine the interests in expression in view of the alternative framework. The free flow of scientific information provides new technologies such as encryption software that allow individuals to more freely communicate in a confidential manner. By requiring individuals to disclose private keys that mask their communications, NSA policies may chill expression in wide range of forums. EES undermines individual expression in that government monitoring raises "big brother" concerns. Required disclosure of keys may make it easier for the NSA to "spy" on individuals because it holds the private keys messages encrypted through use of EES. As such, in the future courts may be in a position to strike down EES as an impermissible form of compelled speech that also contravenes privacy rights.

### 2. Format Discrimination

58. ITAR enforcement also restricts exports of encryption source code in software form that has been previously published in book form and approved for export. As such, restrictions on software exports as opposed to exports of encryption in print may limit individual expression and undermine core values. The NSA justifies differential treatment of software and print by arguing that software provides each source code listing in its own file with the capability of being compiled into multiple routines and copies and that the source code was of such a strategic level as to warrant continued control.[108] Under ITAR, the NSA does not prohibit printing or the distribution of source code to individuals. It does prohibit the distribution of source code on a floppy disk or distribution over the Internet whereby users would be able to download the programs.

59. This distinction may be seen as impinging on free speech because it forecloses software developers from exploiting the full potential of the programs that they develop. It also may be both an arbitrary and capricious application of ITAR. The NSA argues, however, that it has consistently made the distinction between information and technical data in print form as opposed to software. Software distribution over the Internet, in particular, raises concerns that wider channels of distribution make it more likely that the source code will be accessed by governments or criminals. Also, as noted by the NSA, software is more readily copied in usable form and as such poses greater risks for broader use and manipulation than source code in print form.

60. Nonetheless, discriminating against a form of expression where the content is the same as with an unregulated form of expression restricts expression where software is of itself the only meaningful form of distribution for commercial purposes. Given the central free speech interest in protecting the free flow of information, arguments may be made in the future that export controls unfairly limit communications that in other forms are not deemed to jeopardize national security interests. Also, export controls on software may be overbroad and go farther than necessary to serve national security interests because alternative forms of control would serve such interests without absolutely prohibiting distribution. For example, technology currently exists that would allow

software developers to control access to Internet distribution sites. Also, notice mechanisms such as file transfer protocols would display warnings that individuals outside the United States are prohibited from downloading the software.[109]

## V. Conclusion

61. Export control enforcement in the encryption field poses a threat for free speech and scientific expression. In the future as litigants continue to raise free speech objections, courts will be required to develop and reshape free speech doctrines in assessing whether current policies are overbroad or go to far in addressing national security concerns. The NSA's policies in many senses reflect concerns over the transmission of technological ideas of an earlier era rather than the current business environment. As noted by Kenneth W. Dam, "The trade-offs between speech and national security geared toward government controls might have been appropriate during the Cold War are not necessarily appropriate for today's technology-based economy."[110] Today, with the emergence of a globally competitive information economy, policy priorities, in a sense, have reversed, and export controls as well as government industry standards appear to be outdated regulatory devices. Moreover, market forces are clearly moving toward greater software development of encryption source code as well as free distribution over the Internet. As such, the rapid pace of technology development itself make export controls and government standards obsolete. Moreover, the free flow of encryption source codes allows an expanding pool of users to encrypt individual communications and offers private commercial enterprises a worldwide means to safely conduct transactions.
62. The problems associated with applying the appropriate standard of review in the encryption context suggest that courts in the future may look to more general First Amendment values in determining whether governmental controls over encryption technologies are permissible. As such, compelled speech and format discrimination arguments may provide courts with alternative frameworks through which such restrictions may be struck down. Specifically, notwithstanding the uncertain status of the export controls under recent decisions, arguments can be made that source code export controls impermissibly discriminate against software distribution as opposed to encryption in print form, in a manner that limits independent scientific expression as well as the marketplace of ideas.

# Footnotes

[*] Associate at Morrison & Foerster, LLP. University of Virginia, J.D. 1997.

[1] *Abrams v. United States*, 250 U.S. 616, 630 (1919)(Holmes, J., dissenting).

[2] Encryption software can be divided into two categories - private key, or symmetric, encryption systems; and public key, or asymmetric, encryption systems. Private and public key encryption source codes differ in the way in which such information is coded and decoded by the sender and

recipient of information. Symmetric, or private key, encryption source code utilizes the same key to both encrypt and decrypt information. The sender and recipient therefore must both have knowledge of the same private key. In order for a private key system to work effectively, the private key must be limited to the sender and the recipient. Otherwise, anyone else who gains access to the key would be able to decipher the encrypted message, thereby compromising the parties' confidentiality. Currently, private key source code is used extensively for military, intelligence and financial applications. *See* Simson Garfinkel, *PGP: Pretty Good Privacy* 45 (1995). Primarily due to the secure key distribution problems associated with private key encryption, experts in the field of source code developed public key source code in the 1970s. Public key, or asymmetric, source code utilizes two different keys to encode and decode information. One key (the public key) is used to encrypt a message and can be made publicly available to those desiring to communicate in a confidential manner with a specific party. In turn, that specific party is the only holder of the other key (the private key), which is then utilized to decrypt the message.

Because of the advantages of having two keys rather than one, public key source code is now considered to be the standard for computer networks. *See* Dan Lehrer, *Clipper Chips and Cypherpunks,* The Nation, Oct. 10, 1994, at 376. Most source code systems in existence today and most new payment systems devised for on-line commerce utilize public key source code. *See* Rochelle Garner, *Fear and Loathing on the World Wide Web,* Computerworld, Apr. 29, 1996, at 28; Anne Knowles, *Electronic Commerce: Securing Transactions over the Net*, PC Week, Oct. 30, 1995, at 102.

[3] *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip and the Constitution*, 143 U. Pa. L. Rev. 709, 713 (1995)(defining source code).

[4] *See* Gary H. Anthes, Standard Encryption Vulnerable to Attack: Banking's Most Trusted Technique for Funds Transfer Questioned, Computerworld, Feb. 12, 1996, at 6.

[5] *See Information Infrastructure Task Force, NII Security: The Federal Role 1* (draft report June 5, 1995) (citing <http://nsi.org/Library/Compsec/nii.txt>.)

[6] 945 F. Supp. 1279(N.D. Cal. 1996)*, aff'd on reh'g,* LEXIS 13146 (N.D. Cal 1997) (reaching similar holding as applied to regulations implemented by U.S. Department of Commerce).

[7] 925 F. Supp. 1(D.D.C. 1996)*, remanded*, No. 96-5121, 1997 U.S. App. LEXIS 2123, at *1 (D.C. Cir. Jan 1997) (for consideration of transfer of regulatory authority to U.S. Department of Commerce).

[8] 945 F. Supp. at 1290.

[9] 925 F. Supp. at 11.

[10] S. 377, 105th Cong. (1997); S. 909, 105th Cong. (1997); H.R. 695, 105th Cong. (1997).

[11] *See* Lehrer, *supra* note 2.

[12] For an extensive review of the origins of export controls, *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 Law & Com. Reg. 469, 471-81 (1994); Evelyn Richards, *U.S. Plan to Restrict Encryption Software Exports Draws Protests*, Wash. Post, Nov. 14, 1991, at B11. Germany and Switzerland routinely permit the export of high level encryption source code; *see* Evans, *supra* at 482; *see also* Julie Bort & Martin Cheek, *The*

*Eagle Is Grounded: U.S. Software Firms Desperate to Export Encrypted Software Are Being Cramped by the National Security Administration*, Computer Wkly., Feb. 11, 1993, at 32. Although France permits the export of encryption source code, private use of source code is not permitted, and any other use of an encryption program requires the user to provide the government with an encryption key; *see* Evans, *supra* at 482. In the United Kingdom, exports of encryption source code that is generally available is freely permitted (this does not include encryption source code with military applications); *id.*; *see also* Bort & Cheek, *supra* at 32. In Japan and Korea, governmental policy actively promotes rather than discourages exports of encryption source code as a means to advance technological development; *see* Shahid Alam, *Restructuring the United States' Export Legislation for the Post Cold War Era*, 18 Fletcher F. World Aff., 137, 143 (1994)(noting differences between technology policy generally in Japan and Korea as opposed to the United States). The COCOM Industrial List of "dual-use" technologies such as software and technical data banned the export of specified encryption products to the Soviet Union, the Warsaw Pact, and the People's Republic of China. *See* John F. McKenzie, *Implementation of the Core List of Export Controls: Computer and Software Controls*, 5 Software L.J. 1, 1 (1992).

In the wake of the fall of communism in the Soviet Union and Eastern Europe in 1990, COCOM reduced the Industrial List that, in revised version, the United States adopted in August, 1991, as the Commerce Control List (CCL). 15 C.F.R. §774 (Supp. I 1997).

[13]Export Administration Act of 1979, Pub. L. No. 96-72, 93 Stat. 503 (codified as amended in 50 U.S.C. app. §§ 2401-2420 (1994)).

[14]*See* Stephen G. Gould, Secrecy: Its Role in National Scientific and Technical Information Policy, Lib. Trends, Summer 1986, at 72.

[15]*See* 50 U.S.C. § 2402(2)(A).

[16]*See* 50 U.S.C. § 2415.

[17]*See* 15 C.F.R. §§ 768-774 (1997).

[18]The sixteen other nations include Australia, Belgium, Canada, Denmark, France, the Federal Republic of Germany, Greece, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Spain, Turkey, and the United Kingdom.

[19]*See* Arms Export Control Act § 38, 22 U.S.C. § 2778 (1988).

[20]*See* 22 U.S.C. § 2778(a)(1)(1988).

[21]15 C.F.R. 774, (Supp. II) (1997); *See also* 22 C.F.R. § 121.1 Category XIII(b)(1)(1997). The NSA is actively involved in enforcing source code export controls as the State Department refers to NSA expertise in determining what cryptographic items to include on the USML. *See* John P. Barlow, *Decrypting the Puzzle Palace*, Comm. ACM, July 1992, at 25, 27. The NSA continues to include cryptographic technology on the USML and, consequently, the State Department requires encryption exporters to apply for export licenses through the Commodity Jurisdiction procedure. Currently, the NSA requires export licenses for certain encryption source code that contains a high level of encryption as measured by the bits; any software with algorithms of 56 bits or more requires a license. Maximum penalties for violating export licensing requirements for encryption source code range from a one million dollar criminal penalty and ten years in prison to a five-hundred thousand dollar civil penalty and a three year export ban. *See* Evans *supra* note 12, at 480

(citing Steve Higgins, *Breaking U.S. Encryption Statute Could Be Costly*, PC Wk., Feb. 8, 1993, at 1); *see also* 22 U.S.C. 2778 (c)(1988), 50 U.S.C. 2410 (c)(1988).

[22] *See* Evan R. Berlack & Cecil Hunt, *Overview of U.S. Export Controls*, in Coping With U.S. Export Controls 1994, 11, 25 (PLI Com. Law & Practice Course Handbook Series No. A-705, 1994).

[23] *See* 22 C.F.R. 120.5 (1994).

[24] *See* 22 C.F.R. 120.4 (1994).

[25] *See* Steven Levy, *Wisecrackers*, Wired, Mar. 1996, at 196; l42 Cong. Rec. S4619-01, S4624 (daily ed. May *2*, 1996) (statement of Sen. Burns); Garfinkel, *supra* note 2, at 57.

[26] The Clipper Chip contains, in hardware form, a classified government algorithm known as SKIPJACK. It is based on a private, or symmetric, key system. The SKIPJACK algorithm was originally developed by the U.S. government to replace an outdated algorithm known as DES. SKIPJACK is sixteen million times stronger than DES and is virtually unbreakable and would require "400 billion years using today's computer power" to break. *See* Lehrer, *supra* note 2.

[27] The National Institute of Standards and Technology (NIST) issues Federal Information Processing Standards (FIPS) pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949, as amended by the Computer Security Act of 1987. *See* 40 U.S.C. 759(d) (1994); 15 U.S.C. 278g-3 (1994). FIPS are standards and industry guidelines that the NIST promotes to improve the federal government's management of its computers and information technology. *See* Department of Commerce, *Semiannual Agenda of Regulations*, 59 Fed. Reg. 57372(1994). FIPS also set national norms in emerging technology areas where NIST decides such standards benefit industry. While FIPS only apply to federal agencies and government contractors, they often are adopted as national standards by industry. *See* Mitch Ratcliffe, *Security Chips Trigger Alarm: Clipper and Capstone Open Digital Back Door*, Macweek, April 26, 1993, at 1. As such, NIST creates "non-legislative rules" by setting government purchasing standards that indirectly apply to the broader market. "Nonlegislative rules" are not rules per se because there is no grant of congressional authority to the agency in question. Rather, an agency can indirectly create rules by creating standards for government agencies that industry must, due to scale of government procurement in particular industries, adopt as well. *See* Michael Asimow, *Nonlegislative Rulemaking and Regulatory Reform*, 213 Duke L.J. 381, 383 (1985).

Attempting to promote universal acceptance of government designed encryption source codes that can be deciphered in order to standardize domestic and international use of such codes, the NSA has promoted a key escrowed encryption source code known as the Escrowed Encryption Standard (EES) which theoretically will make it easier for the NSA to monitor Internet communications as well as access computer stored information. EES involves three keys: the session key, the chip key, and the family key. *See supra* note 2 and accompanying discussion. If an individual communicates by the Internet with another individual with corresponding equipment, both individuals select a session key. The session key is then transmitted by a process which sends a data stream known as a Law Enforcement Access Field (LEAF). EES encrypts the LEAF data with a unique chip key and then reencrypts the data with the family key, which is held by the government. *See* Evans, supra note 12, at 757 (outlining how the three key system works in practice)

[28] *See* National Inst. of Standards & Technology, Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997 (1994) (hereinafter "Final EES Approval").

[29] The three key source code system is designed to create a number of procedural safeguards in order to protect the privacy of legal communications while at the same time providing easy access and monitoring when required. Evans, *supra* note 12, at 758 (noting procedural safeguards). If a monitoring agency targets criminal or security related EES communications or computer stored information, it is able to only record the LEAF data. The agency must then acquire the family key which will be stored in special circuit boards that can be used in computers at various agencies. Once the agency acquires the family key, it can decrypt the LEAF data in order to discover the unique chip key. Finally, the security agency is required to contact two escrow agencies and provide them with the unique chip key information and a warrant from a state or federal court authorizing the security agency to decrypt the communications or computer stored information. The escrow agents have no duty to assess the merits of the request but will only check the validity of the warrant. If the warrant is legitimate, the escrow agents are required to disclose the session key segments for the unique chip key identified by the security agency. With the decrypted session key, the security agency is able to decrypt the communications.

Consequently, the government source code standard allows individuals to protect their communications while still allowing for government monitoring based on procedural safeguards. Under current NSA policy, NIST and the Treasury Department's Automated Systems Division serve as the escrow agents who possess the key segments and issue each unique key. The escrow agents will have the additional responsibility of protecting each chip's or card's unique key from rogue security agents and ensuring the security of the key generation process. By requiring that all government purchased computers contain EES, the NSA anticipates that the volume of business the government generates will force encryption source code developers to use EES for non-governmental applications as well.

[30] *Final EES Approval*, *supra* note 28, at 6001.

[31] 354 U.S. 476, 487 (1957).

[32] 413 U.S. 15, 34 (1973).

[33] 438 U.S. 726, 746 (1978).

[34] *See, e.g., Aptheker v. Secretary of State*, 378 U.S. 500, 509 (1964); *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 558 (1975). For a general review of national security arguments, *see* Kenneth J. Pierce, *Public Cryptography, Arms Export Controls, and the First Amendment: A Need For Legislation*, 17 Cornell Int'l. L.J. 197, 211 (1984); *see also Developments in the Law: The National Security Interest and Civil Liberties*, 85 Harv. L. Rev. 1130, 1274-75 (1972).

[35] 925 F. Supp. At 10, 11. Under the *O'Brien* test, a prior restraint on speech is permissible if it serves such an interest and at the same time is not overbroad. A government prior restraint is permissible "if (1) it is within the government's power; (2) furthers an important or substantial government interest; (3) if the governmental interest is unrelated to the suppression of free expression; and (4) if the incidental restriction on alleged First Amendment freedoms is no greater

than is essential to the furtherance of that interest." *United States v. O'Brien*, 391 U.S. 367, 377 (1968); *see also* John H. Ely, *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*, 88 Harv. L. Rev. 1482, 1483-84 (1975).

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

[37] *Id.* at 4.

[38] *Id.* at 11, 12.

[39] *Id.*

[40] *Id.*

[41] *Id.* at 11. ("This 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.").

[42] *Id.* at 11, (citing *Chicago & Southern Airlines v. Waterman S.S. Corp.*, 333 U.S. 103 (1948)).

[43] *Id.* at 13 (citing *Ass'n of Accredited Cosmeteology Schools v. Alexander*, 979 F.2d 859, 866 (D.C. Cir. 1992)).

[44] 925 F. Supp. at 13.

[45] 369 U.S. 186 (1962).

[46] 904 F.2d 601, 602 (5th Cir. 1990).

[47] 922 F. Supp. at 1426.

[48] *Id.* at 1430.

[49] *Id.*

[50] *Id.*; *see also supra* note 29 and accompanying discussion.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.* at 1434 (citing *Sweezy v. New Hampshire*, 354 U.S. 234, 249-50 (1957))(noting the importance of protecting scholarship and academic inquiry).

[55] *Id.* at 1436.

[56] *Id.* at 1438; *see also Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1973); *Vance v. Universal Amusement Co.*, 445 U.S. 308, 317 (1980); *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971).

[57] 583 U.S. 697 (1931).

[58] *Id*. Exceptions, for example, include obstruction of military recruiting, publication of the sailing dates of military transports or of the number and location of troops; publication of obscene matter, and incitements to violate or forcibly overthrow the government.

[59] *See generally*, James Ferguson, Scientific Inquiry and the First Amendment, 64 Cornell L. Rev. 639 (1979); Harold Relyea, Silencing Science: National Security Controls and Scientific Communication 38 (1994).

[60] 925 F. Supp. at 6.

[61] 922 F. Supp. at 1437-39.

[62] 369 U.S. at 217.

[63] 249 U.S. 47, 52 (1919).

[64] *See* Barlow, *supra* note 21, at 25, 27.

[65] *Id.*

[66] *See generally id.; Bernstein*, 922 F. Supp. at 55.

[67] 22 C.F.R. § 120.10 (1996).

[68] 467 F. Supp. 990 (W.D. Wis. 1979), *dis. Without op.*, 610 F.2d 819 (7th Cir. 1979)

[69] *See generally*, New York Times Co. v. United States, 403 U.S. 713 (1971).

[70] 380 U.S. 51 (1965).

[71] *Id.* at 58-61.

[72] 610 F.2d 819 (7th Cir. 1979); *see generally* L.A. Powe Jr., *The H-Bomb Injunction,* 61 U. Colo. L. Rev. 55 (1990).

[73] 467 F. Supp. at 991.

[74] *See* John Schwartz, *Privacy Program: An On-Line Weapon?*, Wash. Post, Apr. 3, 1995, at Al.

[75] Current NSA policy may prevent U.S. companies from distributing encryption source code that is freely available notwithstanding export controls on their products. Consequently, foreign companies are freely permitted by their respective governments to distribute their equivalent technology in the markets in which they compete with U.S. companies. *See Privacy Issues in the Telecommunications Industry: Hearings on the Administration's "Clipper Chip" Key Escrow Encryption Program Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary*, 103rd Cong., 2d Sess. (May 3, 1994).

[76] *See* Froomkin, *supra* note 3, at 750 (citing the URL at <ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/pgp/2.6mit>).

[77] The federal government has emphasized that, although sophisticated encryption is available abroad, limiting distribution serves a national security interest by reducing the difficulties created for federal agencies when encountering high level encrypted communications or transactions. For instance, FBI Director Louis Freeh has argued that the government retains an interest in controlling the distribution of encryption source codes because of the costs associated with unmonitorable forms of communication. *See The Promotion of Commerce On-Line In The Digital Era (Pro-CODE) Act of 1996: Hearings on S. 1726 Before the Science, Technology and Space Subcomm. of the Senate Comm. on Commerce, Science & Transportation, Science*, 104 Cong., 2nd Sess. (1996)("The experience of our own agencies here in the United States, for instance, tell us that with 56-bit encryption, using all of the supercomputers available, my agents would need one year and 87.5 days to decrypt one message. That is not timely, that is not safe.").

[78] 22 C.F.R. § 120.17(1),(4) (1996).

[79] 579 F.2d 516, 521 (9th Cir. 1978).

[80] *Id*.

[81] *Id*.

[82] *See generally* Kenneth W. Dam, *the Cryptography Wars*, Wash. Post, July 23, 1996, at A17.

[83] *See id.*

[84] *Id*. Given the significant disadvantages for U.S. technology corporations created by export

controls, others have argued that such controls may needlessly damage U.S. competitiveness in an emerging business area where global competition is fierce. Export controls also unnecessarily constrain U.S. software companies in competing against their foreign counterparts, which are able to sell products with higher level encryption. Foreign competitors are free to export encryption source code higher levels than those permitted by the U.S. government under current export controls. *See Encryption: Bipartisan Senate Coalition Backs Bill to Lift Source Code Export Restrictions,* BNA Int'l Trade Daily, May 6, 1996. Jim Barkedale, President and CEO of Netscape Communications Corp., has commented that foreign competitors are even using U.S. export control laws as an explicit part of their marketing strategy. As security becomes the basis for many purchasing decisions, export controls on strong encryption jeopardize American leadership in enormously promising, but rapidly changing high-tech industries like the Internet industry. *See The Promotion of Commerce On-Line In The Digital Era (Pro-CODE) Act of 1996: Hearings on S. 1726 Before the Science, Technology and Space Subcomm. of the Senate Comm. on Commerce, Science & Transportation, Science*, 104th Cong., 2nd Sess. (1996)(statement of Jim Barksdale, President and CEO of Netscape Communications). Also, export restrictions may encourage U.S. high-tech companies to relocate their production facilities outside of the United States in order to avoid export control enforcement and this could further undermine U.S. competitiveness. *See id*. Furthermore, the diluted level of encryption source code that can be exported under ITAR may become the standard for software sold domestically and thus reduce the potential for the industry over-all. For example, while Netscape releases both a 128-bit domestic version and a 40-bit international version, many software companies simply avoid the costs of creating and updating separate versions of their software by releasing a single version. *See* John J. Fialka, *United States Strategy Should Promote Computer Codes,* Wall St. J., May 31, 1996, at B5. Promotion of the EES standard in the United States, like export controls on encryption source code, risks undermining the competitiveness of the U.S.-based encryption source code industry. As encryption capabilities become increasingly important and move toward software applications, EES may reduce the investment incentives for U.S. software developers to create encryption source code products. *Id.*

[85]Vannevar Bush, *Science - The Endless Frontier*, 29 U.S. Office of Scientific Research and Development, National Science Foundation (1980).

[86]For instance, Justice Brandeis applied the marketplace of ideas rationale for free speech in broadening protection of free thought and expression, and argued that free speech was a "means indispensable to the discovery and spread of truth." *Whitney v. California*, 274 U.S. 357, 375-76 (1927)(Brandeis, J., concurring).

[87]*See, e.g.,* Harold Green, *The Boundaries of Scientific Freedom,* J. of Sci., Tech., and Human Values, June 1995, at 17.

[88]299 N.Y.S.2d 551, 557 (Sup. Ct. 1969).

[89]Vincent Blasi, *The Checking Value of First Amendment Theory,* 530 Am. Found. Res. J. 523, 550 (1977).

[90]*See* Carl L. Becker, Freedom and Responsibility in the American Way of Life 31 (1947).

[91]Lawrence Solum, Freedom of Communicative Action: A Theory of the First Amendment Freedom of Speech, 83 NW. U. L. Rev. 54, 77 (1989); see also Frederic Schauer, Free Speech: A

Philosophical Enquiry 16 (1982).

[92] Martin Redish, *The Value of Free Speech*, 130 U. Pa. L. Rev. 591, 628 (1982).

[93] *See* Ferguson, *supra* note 59, at 639.

[94] *See* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 761-65 (1976).

[95] Joseph Bowman, *Jefferson's "Freedom of Speech" from the Standpoint of Science,* 82 Science 529 (1935). In a sense, Jefferson's interest in the free expression of scientific ideas trumped his devotion to political discourse. Lawrence Levy has noted that Jefferson's "threshold of tolerance for hateful political ideas was less than generous while he cared more deeply for the intellectual liberty of religious, scientific or philosophical heretics." *See* Lawrence Levy, *Jefferson as a Civil Libertarian*, in *Thomas Jefferson: The Man...His World...His Influence* 197 (L. Weymouth ed. 1973).

[96] *Riley v. Nat'l Fed'n of the Blind*, 487 U.S. 781, 795 (1988); *see also* Froomkin, *supra* note 3, at 726.

[97] 487 U.S. at 789.

[98] 430 U.S. 705, 713 (1977).

[99] *See Buckley v. Valeo*, 424 U.S. 1, 64 (1976).

[100] *See Final EES Approval*, *supra* note 28, at 6005; *see also* Froomkin, *supra* note 3, at 766.

[101] EES simply states that "various devices implementing this standard are anticipated. The implementation may vary with the application. The specific electric, physical and logical interfaces will vary with the implementation." *Final EES Approval*, *supra* note 28, at 6001. Consequently, the NRC Report referred to U.S. encryption source code export restrictions as "a policy morass which has stifled innovation, limited the availability of strong, easy to use encryption technologies, and endangered the ability of U.S. companies to compete in the global information marketplace." *See* Center for Democracy & Technology, *NRC Report Calls Administration Crypto Policy Into Question*, CDT Policy Post, May 30, 1996. Specifically, the NRC called for dismantling export controls since the widespread use of encryption by private businesses and individuals is inevitable. As part of its recommended "judicious transition," the panel advised specifically that the government should permit the export of software with a 56-bit or more algorithm. *See* Fialka, *supra* note 84, at B5.

[102] *See* Robert A. Anthony, Interpretative Rules, Policy Statements, Guidances, Manuals, and the Like: Should Federal Agencies Use Them to Bind the Public? 41 Duke L. J. 1311, 1333-40 (1992).

[103] *See* Froomkin, *supra* note 3**,** at 770.

[104] Government purchases of EES computers or telephones are often funded through appropriations that do not require congressional approval. For example, the Department of Justice acquires computers by drawing from its Asset Forfeiture Super Surplus Fund which includes profits from RICO enforcement; *see* Froomkin, *supra* note 3, at 770.

[105] *Id.* at 771.

[106] *Final EES Approval, supra* note 28, at 6000.

[107] *See* Lehrer, *supra* note 2 ("a little encryption box that can be attached to any phone,

computer or TV set and used as an alternative encryption program, like P.G.P., to scramble data before it hits Clipper. A smart kid with $50 to spend on hardware could securely encrypt a telephone conversation.")

[108] *See* Froomkin, *supra* note 3, at 751.

[109] Edward Radlo, *Legal Issues in Cryptography*, Computer Law., May 1996, at 7.

[110] *See* Dam, *supra* note 82.