Harvard Journal of Law & Technology
Volume 10, Number 3 Summer 1997

CRYPTOGRAPHY, EXPORT CONTROLS, AND THE FIRST AMENDMENT IN *BERNSTEIN V. UNITED STATES DEPARTMENT OF STATE*

Thinh Nguyen[*]

TABLE OF CONTENTS

I. INTRODUCTION

In *Bernstein v. United States Department of State*,[1] the District Court for the Northern District of California ruled that licensing requirements for the export of cryptographic software under the International Traffic in Arms Regulations ("ITAR") an unconstitutional prior restraint of protected speech.[2] On its face, this decision appeared to be a victory for those who advocate curtailing export controls on cryptographic technology in order to ensure academic freedom and to promote greater individual privacy and business security on communications networks. It raised serious concerns to others, particularly police and national security officials, who view the widespread dissemination of electronic

* J.D., Harvard Law School, Class of 1999.

1. 945 F. Supp. 1279 (N.D. Cal. 1996), *enforcing* 922 F. Supp. 1426 (N.D. Cal. 1996) (ruling that computer code was protected speech under the First Amendment).

2. *See id.* at 1292.

cryptography as one of the greatest emerging threats to our nation's law-enforcement and intelligence-gathering capabilities.

This Note does not attempt to resolve this dispute, but rather seeks to identify key issues in the *Bernstein* decision in which the emerging global information infrastructure challenges the coherence of the doctrinal approach taken by the court. Part II summarizes the growing conflict between promoting the widespread use of cryptography and protecting law enforcement and national security objectives. Part III discusses the *Bernstein* decision and subsequent regulatory actions by the Clinton administration. Part IV argues that the Bernstein court's analysis of First Amendment issues and its definition of "export" reveal a basic confusion about the technologies on which the debate centers. This Note concludes with the need to reframe these doctrinal and policy questions to take into account the technical realities and market forces, as well as potential dangers, of the information society.

II. CRYPTOGRAPHY AT THE CROSSROADS

A. Military and Law Enforcement Perspectives

For millennia, people have employed cryptography as a tool for securing communications, and for equally as long, other people have tried to decode those messages.[3] During World War II, the Allies were able to break a secret German code, called Enigma.[4] With this capability, they were able to locate and sink large numbers of German U-boats and obtain advanced information about German military operations that was critical to the campaign in Europe.[5] Similar code-breaking ability also allowed the United States Navy to intercept the Japanese fleet in one of the most decisive battles in the Pacific — the Battle of Midway.[6] During the Cold War, signals intelligence provided information about the Soviet Union's military capabilities, the downing of Korean Airlines Flight 007, and Libyan involvement in the bombing of the La Belle Discotheque in West Berlin.[7] More recently, intercepted communications have been used to reveal unfair trading practices by competing nations, monitor proliferation of weapons of mass destruction, enforce

---

3. *See* Deborah Russell & G.T. Gangemi, Sr., *Encryption*, *in* BUILDING IN BIG BROTHER: THE CRYPTOGRAPHY POLICY DEBATE 10, 11 (Lance J. Hoffman ed., 1994).

4. *See id.* at 14.

5. *See* COMMITTEE TO STUDY NATIONAL CRYPTOGRAPHY POLICY, NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 96-97 (1996) [hereinafter NRC REPORT].

6. *See* DAVID KAHN, THE CODEBREAKERS 561-73 (1967).

7. *See* NRC REPORT, *supra* note 5, at 98-99.

international sanctions, identify conventional military threats, and prevent terrorism.[8]

The growing prevalence of computers could rapidly put an end to this capability. The strength of any encryption depends on how rapidly it can be decrypted.[9] The only known method which can be mathematically proven to be unbreakable is the one-time cipher.[10] Other methods rely on having a reusable "key," which generates a series of substitutions or transpositions of the original message (called "plaintext") to create a coded message ("codetext" or "ciphertext"). This codetext can be sent to the recipient, who has an identical or complementary key that can be used to reverse the process ("decrypt") and produce the original plaintext.[11] Because the one-time cipher is difficult to use (the main problem is continuous and timely key distribution), most cryptographic systems use transposition or substitution ciphers, which are theoretically breakable.[12]

All cryptographic systems other than the one-time cipher use mathematical formulas to generate the ciphertext from the plaintext using a key. Someone who intercepts the ciphertext cannot understand it without breaking the code. One way to do this, assuming one knows the formula used to encrypt, is to try every possible key combination until one obtains a readable text (a process called "brute-force" search).[13] Such methods are quite successful if the key is short, but as the key becomes longer (e.g., by adding more binary digits, or bits, to the key), the time for such a search grows exponentially. For a sufficiently large key, a brute-force search on even the most powerful supercomputer could take longer than the life of the universe.[14] More sophisticated ways to the find the correct key are available for various cryptographic systems, but in principle, the sender can always increase the key size until the search time for any would-be codebreaker becomes prohibitively long.[15] Since the cost of brute-force searching grows far more

---

8. *See id.*
9. *See* Russell & Gangemi, *supra* note 3, at 15.
10. *See id.* at 22.
11. *See id.* at 16.
12. *See id.* at 22.
13. *See* NRC REPORT, *supra* note 5, at 63.
14. *See id.* (noting that for every additional bit added to the key size, the search time doubles). If a computer can try a million different combinations a second, it would take it about 11.5 days to break a 40-bit key and over 2,000 years to break a 56-bit key. *See id.*
15. One common encryption formula, called RSA, generates encryption keys by multiplying two very large prime numbers together. The problem for code-breaking is reversing this multiplication process (a process called factoring). However, factoring a large number can take a long time, even on the most powerful computers. Therefore, it is much easier to encrypt than to reverse the process without knowing one of the prime numbers (i.e. the key). Currently, an RSA key of 230 bits is considered beyond the power of any

rapidly than the cost of encryption with longer keys, the capability to obtain practically unbreakable encryption is becoming commonplace as the consumer computer market supplies increasing speed at lower cost.[16] Even imperfect encryption, if widely used, could raise the costs of systematic interception tremendously. Thus, the convergence of computers and cryptography is threatening one of the most cherished capabilities of both national security and law enforcement communities: the ability to eavesdrop on criminal or hostile communication.

B. Individual Privacy and Business Security

The desire for individual privacy and the need for secure business transactions are at the same time creating increasing market demand for better cryptography. U.S. companies are common targets for economic espionage, often by foreign intelligence services.[17] According to a National Counterintelligence Center report, unauthorized interceptions of business communication "account for the largest portion of economic and industrial information lost by U.S. [c]orporations."[18] As an attempt in 1994 to steal $12 million from Citicorp by an international group of criminals demonstrated, banks and financial institutions require better abilities to authenticate transfers as money increasingly moves through computerized networks.[19] Because cryptography can ensure confidentiality, integrity, and authenticity in day-to-day communication, it is well-suited to fill these needs.[20]

As more people use the Internet and other networks, they are entrusting ever growing amounts of personal information to these systems. Yet without the ability to encrypt communication, many of these systems, including the Internet, are highly vulnerable to eavesdropping, clandestine alteration of data, and other manipulation by third parties.[21] For example, transmitting credit card numbers over the Internet is quite risky.[22] As these forms of communication grow, individuals and organizations will increasingly displace the federal government as the primary consumers of cryptographic software.[23] This market demand for

---

computer to factor within a reasonable time and is thus presumed to be secure. *See* Richard E. Crandall, *The Challenge of Large Numbers*, SCI. AM., Feb. 1997, at 74, 75.

16. *See* NRC REPORT, *supra* note 5, at 380-81.
17. *See id.* at 32-33.
18. *See id.* at 31.
19. *Id.* at 23.
20. *See* Russell & Gangemi, *supra* note 3, at 16.
21. *See* NRC REPORT, *supra* note 5, at 24.
22. *See id.* at 41.
23. *See id.* at 29-30. For a thorough discussion of potential uses of cryptography by private individuals, see *id.* at 42-46.

cryptography collides with the objectives of law-enforcement and national security agencies who have traditionally kept tight reins on cryptographic technology.

III. THE *BERNSTEIN* DECISION

A. Export Regulations

In 1995, Daniel Bernstein, a graduate student in mathematics at the University of California at Berkeley, filed suit in the District Court for the Northern District of California seeking declaratory judgment against the Department of State to prevent it from enforcing the Arms Export Control Act ("AECA"),[24] and ITAR.[25] Bernstein wrote an encryption algorithm called "Snuffle" as part of his graduate research.[26] Bernstein wanted to publish this work, present it at technical meetings, and teach it in his classes.[27] But after receiving advice from colleagues that he might inadvertently violate export regulations by undertaking these activities, he decided to submit his research to the Office of Defense Trade Controls ("ODTC") of the Department of State, for a "commodity jurisdiction"[28] determination.[29] The commodity jurisdiction request is a procedure available under ITAR to determine whether a given item falls under the United States Munitions List, and is thus subject to controls.[30] If an item is on this list, it requires a license before it can be exported.[31] Because ITAR defines "export" to include "disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad,"[32] Bernstein was concerned that he might have been criminally liable under ITAR for publishing his algorithm, placing it on an Internet web-page for his classes, or even teaching it in a class with foreign nationals.[33]

The ODTC informed Bernstein that the "Snuffle" program was a "defense article" under Category XIII(b) of the Munition List and was

---

24. Arms Export Control Act of 1976 § 38, 22 U.S.C. § 2778 et seq. (1994).
25. International Traffic in Arms Regulations, 22 C.F.R. § 120 et seq. (1996).
26. *See* Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996).
27. *See id.* at 1430.
28. *See* International Traffic in Arms Regulations, 22 C.F.R. § 120.4(a) (specifying a procedure for determining if an article is covered under the Munition List).
29. *See id.*
30. *See* International Traffic in Arms Regulations, 22 C.F.R. § 121 (1996).
31. *See* NRC REPORT, *supra* note 5, at 116.
32. International Traffic in Arms Regulations, 22 C.F.R. § 120.17(a)(4) (1996).
33. *See Bernstein v. United States Dep't of State*, 945 F. Supp. 1279, 1296 (N.D. Cal. 1996).

subject to export licensing requirements.[34] Unsure of whether this included his academic papers, he submitted a second commodity jurisdiction request asking for a separate ruling on each component of the research, including: (1) the paper, "The Snuffle Encryption System"; (2) source code for the encryption program; (3) source code for the decryption program; (4) an English description of the algorithm; and 5) an English description of how the procedure functions.[35] ODTC notified Bernstein three months later that *all* of the items were subject to controls.[36] After Bernstein filed suit seeking declaratory judgment, the ODTC reversed itself and informed him that its decision applied only to the source codes.[37]

B. Computer Code as Protected Speech

In a preliminary ruling, Judge Marilyn Patel denied the government's motion to dismiss for lack of justiciability,[38] and held that cryptographic computer source code is speech. Thus, Bernstein had asserted a "colorable" claim to First Amendment protection.[39] The court thus became the first to recognize a protected speech interest in computer code.

The court noted in dicta that "the paper, an academic writing explaining the plaintiff's scientific work . . . is speech of the most protected kind."[40] However, the only remaining issue was whether the source code deserved protection as speech.[41] The government argued that source code was conduct not speech, citing *Texas v. Johnson*,[42] in which the Supreme Court held that flag burning is conduct. However, the *Bernstein* court pointed out that the conduct/speech analysis is proper only in the absence of "the spoken or written word."[43] The court pointed out that "Bernstein's encryption system is written, albeit in computer language."[44] The court also noted that "[a] computer program is so

---

34. *See* International Traffic in Arms Regulations, 22 C.F.R. § 121.1 XIII(b)(1) (1996) (including, as defense articles, "cryptographic (including key management) systems, equipment . . . or software with the capability of maintaining secrecy or confidentiality of information or information systems," but exempting decryption-only systems, banking applications, and analog scrambling).

35. *See Bernstein*, 945 F. Supp. at 1284.

36. *See id.* at 1285.

37. *See id.*

38. *See id.* at 1439.

39. *See id.* at 1437.

40. *Id.* at 1434.

41. *See id.* at 1434.

42. 491 U.S. 397 (1989).

43. *Bernstein*, 922 F. Supp. at 1434 (quoting *Johnson*, 491 U.S. at 404 (1989)).

44. *Berstein*, 922 F. Supp. at 1435.

unlike flag burning and nude dancing that defendants' reliance on conduct cases is mistaken" and observed that "[t]his court can find no meaningful difference between computer language, particularly high-level languages as defined above, and German or French."[45] Therefore, the court reasoned, computer code operates as a language that can communicate ideas. It was of no relevance whether those ideas were "functional" or even whether the code "'communicates' to and directs [an] instrument itself," rather than a living person.[46]

In a subsequent opinion, the court held that the licensing requirement for cryptographic software under Category XIII(b) of the Munitions List was an unconstitutional prior restraint of speech, noting that "even if a government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not condition that speech on obtaining a license or permit from a government official in that official's boundless discretion."[47] The court ruled that the "Snuffle" source code was itself protected speech.[48] Thus, the court did not need to reach Bernstein's argument that there is a First Amendment interest in speaking confidentially and therefore his software should be protected because it facilitates this security.[49]

Since Category XIII(b) is "directed very specifically at applied scientific research and speech on the topic of encryption,"[50] it aims at expression itself rather than the manner of expression, the court reasoned. Absent the threat of "direct, immediate, and irreparable damage to our Nation or its people," the government cannot justify prior restraint on speech.[51] The court also observed that "[t]he ITAR scheme [is] a paradigm of standardless discretion," that fails to ensure prompt licensing decisions, provide adequate judicial review, or require that licensing officials bear the burden of defending their actions.[52] The court thus ruled that the ITAR licensing system, as applied in Category XIII(B) relating to cryptography is an unconstitutional prior restraint of protected speech in violation of the First Amendment.

For the same reasons, the court also held that the technical data provision of ITAR, which exempts fundamental research and "public

---

45. *Id.*

46. *Id.*

47. *Id.* at 1286 (quoting *Lakewood v. Plain Dealer Pub'g Co.*, 486 U.S. 750, 764 (1988)).

48. *See Bernstein*, 945 F. Supp. at 1287.

49. *See id.*

50. *Id.* at 1288.

51. *Id.* (quoting from Justice Stewart's concurring opinion in *New York Times Co. v. United States*, 403 U.S. 713 (1971), in which the *New York Times* and the *Washington Post* were allowed to publish the Pentagon Papers).

52. *Bernstein*, 945 F. Supp. at 1289.

domain" materials was unenforceable as far as it relates to the Category XIII(b) cryptography provision.[53] Here, Judge Patel looked to *United States v. Edler*,[54] in which the defendant appealed his conviction for unlicensed exportation of a technique of tape wrapping used to build missile components. In *Edler*, the Ninth Circuit ruled that the technical data provision was to be construed narrowly to prohibit export only of items "significantly and directly related to specific articles on the Munitions List,"[55] in order to avoid striking down the entire regulation.[56] While Judge Patel's decision questioned the continuing validity of *Edler* in its dicta, it did not attempt to disturb the precedent. However, since Judge Patel held Category XIII(b) to be unconstitutional, the technical data provision was, for practical purposes, unenforceable against cryptographic devices.[57]

Judge Patel also ruled that the academic exemption for "general scientific, mathematical or engineering principles"[58] was impermissibly vague and failed to provide researchers with "a reasonable opportunity to know what is prohibited."[59] She also struck from the definition of "defense articles" the term "technical data," so as to avoid circular and overlapping definitions of the two terms.[60] However, she did not find that the term "export" was vague (see below for a discussion of this aspect of the ruling).[61]

The net effect of these rulings was to strike out Category XIII(b) of the Munitions List and remove cryptographic technologies from the export control list. Bernstein was free to teach, publish, or even post his programs on an Internet site for his students.[62] Almost immediately, the Clinton Administration acted to close this gap in the export controls regime by transferring all the cryptographic provisions of Category XIII(b) to the Commerce Control List,[63] administered under the Export

---

53. *See* International Traffic in Arms Regulations, 22 C.F.R. § 120.10 (1996).
54. 579 F.2d 516 (9th Cir. 1978).
55. *Id.* at 521.
56. *See Bernstein*, 945 F. Supp. at 1291.
57. *Id.* at 1292.
58. 22 C.F.R. § 120.10(a)(5) (1996).
59. *See Bernstein*, 945 F. Supp. at 1293-94 ("[T]he uncertainty created in scientists about what speech is subject to regulation under the ITAR is unacceptable.").
60. *See id.* at 1293 (referring to 22 C.F.R. § 120.6).
61. *See id.* at 1294.
62. *See id.* at 1296.
63. *See* 61 Fed. Reg. 68,633 (1996) (to be codified at 22 C.F.R. pt. 121) (proposed Nov. 15, 1996).

Administration Regulations[64] of the Department of Commerce,[65] while at the same time revising the regulations to impose essentially the same controls that caused Judge Patel to invalidate the ITAR provisions.[66]

IV. DISCUSSION

A. Speech/Conduct Distinction

The Bernstein court relies on the verbal characteristics of computer source code to find that software itself is more like speech than "conduct." For example, it argues that computer source code is more like "German or French" than like "flag burning and nude dancing."[67] By defining source code as a "language" that serves as a "complex system of understood meanings within specific communities," it is easy to see, the court asserts, that computer language is in fact "speech."[68]

The analysis by the Bernstein court to explain why software is speech instead of conduct is not entirely satisfying, given the momentous import of its ruling that computer source code is a form of protected speech. The distinction between speech and conduct on which the court relies in finding a first amendment protection for computer code been recognized as problematic in other contexts.[69] It is particularly ill-suited

---

64. *See* 15 C.F.R. § 774 (1996).

65. For an explanation of the many subtle differences between export controls under the Export Administration Regulations regime and the ITAR regime, see NRC REPORT, *supra* note 5, at 118-19.

66. *See* 61 Fed. Reg. 68,572 (1996) (to be codified at 15 C.F.R. pts. 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772 & 774).

67. *See* Bernstein v. United States Dept. of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996).

68. *See id.*

69. *See* LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-7 825-832 (2d ed. 1988) (noting that the distinction arises from labor picketing cases such as Thornhill v. Alabama, 310 U.S. 88 (1940) and arguing that the dichotomy is too oversimplified to be applied consistently or to have much determinate content); Cass R. Sunstein, *Words, Conduct, Caste*, 60 U. CHI. L. REV. 795 (1993) (arguing that regulation of speech should be evaluated against goals of fostering democracy and equality, not on the speech/conduct distinction); *see also* Stephanie M. Kaufman, *The Speech/Conduct Distinction and First Amendment Protection of Begging in Subways*, 79 GEO. L.J. 1803 (1990); Paul Reidinger, *The Expressionists: When Is Conduct Speech?* 76 A.B.A. J. 90 (1990) (surveying recent court decisions implementing the speech/conduct distinction); Sally A. Specht, *The Wavering, Unpredictable Line Between "Speech" and Conduct*, 40 WASH. U.J. URB. & CONTEMP. L. 173 (1991); Aviva O. Wertheimer, *The First Amendment Distinction Between Conduct and Content*, 63 FORDHAM L. REV. 793 (1994).

to the realities of computer technology because software inseparably incorporates elements of both expression and function.[70]

One difficulty with this analogy is that traditional languages involve communication between human beings. This idea is crucial for First Amendment analysis. Suppose *A* attempts to convince *B* to do something (say by giving a political speech), and *B*, influenced by the speech, commits a crime. In this case, the causal chain from *A*'s action (the speech) to *B*'s action (the crime) has been mediated through *B*'s reflection on *A*'s speech. To the extent that the crime resulted from an independent exercise of reasoning and judgment by *B* based on the ideas communicated by *A*, *A* will be immune from criminal liability under established First Amendment principles.[71] This is because holding speakers responsible for even foreseeable consequences of their speech would unacceptably chill free expression. By contrast, the whole point of computer source code is that a compiler can translate it into object code (the binary set of instructions on which the computer's processor operates). Compiling source code does not require that the user know or understand the contents of the source code. Furthermore, object code is a tool that, together with a general-purpose computer, can be used to perform specific tasks just like any other physical device. Unless the user is a computer programmer, he is unlikely to care — or perhaps even know — that the genesis of this tool involved expression, any more than the user of a bomb cares about the contents of the blueprints used to build it.[72]

The court avoided this difficulty by drawing a further analogy. It noted that music is protected speech under the First Amendment, and "like source code converted to object code, it 'communicates' to and directs the instrument itself."[73] However, musical melodies are meant ultimately to be heard and interpreted by a human audience. They are not self-executing, but must be interpreted and reconstructed as sound by the listener. In contrast, computer software can serve both roles: it can serve as a medium for information communication (e.g., restructuring

---

70. *Cf.* Arnold H. Loewy, *Distinguishing Speech From Conduct*, 45 MERCER L. REV. 621, 632 (1994) (concluding that symbols deserve as much protection in First Amendment jurisprudence as words).

71. *See* Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (overruling conviction of a Ku Klux Klan leader because criminal syndicalism statute was not directed at activities "inciting or producing imminent lawless action" and "likely to incite or produce such action").

72. Modern computer languages, for example JAVA, developed by Sun Microsystems, can compile and implement high-level source code, once transmitted, without further intervention from a human user. See PATRICK NIEMEYER & JOSHUA PECK, EXPLORING JAVA 4 (1996).

73. Bernstein v. United States Dept. of State, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996).

text and images from binary electronic signals), and it may perform complex actions (e.g., trade on stocks, transfer money, or even direct airplane traffic patterns).

Nor is the speech/conduct dichotomy a useful device for answering myriad questions that arise when we classify software as "speech." For example, would the *Bernstein* court protect people who transmit a computer virus on the Internet using otherwise lawful access?[74] Laws currently make this a crime.[75] Suppose someone does not actively transmit the virus, but leaves it a file on the Internet for others to download and use as they wish. If somehow the virus found its way into the computer systems of a major telephone company and disrupted service — or infiltrated the Department of Justice computers, would the original author be criminally liable? And what if the writer merely published the source code for the virus in a journal? Asking whether the computer virus software contained recognizable "words" and therefore whether it is sufficiently verbal to qualify as speech seems particular irrelevant and fruitless in creating an analytic framework for these problems.

To appreciate the pitfalls, consider a flaw recently discovered in the Microsoft Internet Explorer program that would have allowed someone to damage another's computer (e.g. erase someone's hard drive) over the Internet with a simple command.[76] Suppose someone put a simple command on her web page, consisting of the words "Delete All," which, when triggered by a vulnerable party innocently browsing the page, would wipe the victim's entire hard disk drive. Would the words "Delete All" qualify as speech and therefore be protected, or are they more like conduct?[77] If they are more like "conduct," then what about a complex computer program consisting of a series of such simple commands? As these examples are meant to show, an analysis of computer code using the conduct/speech distinction is problematic in that it is unlikely to resolve numerous issues that immediately arise once we decide to call software "speech."

The problem with the 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. A critical insight into the First Amendment protection of

---

74. *See* Patrick J. Leahy, *New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law*, 5 HARV. J.L. & TECH. 1, 21-22 (1992).

75. *See* Computer Abuse Amendments Act, 18 U.S.C. § 1030(a)(5)(A) (1994) (making "conduct" which is intended to damage a protected computer a crime).

76. *See* Mark Melady, *Microsoft Security Flaw Found*, TELEGRAM & GAZETTE, Mar. 5, 1997, at A1.

77. For examples of simple viruses, Trojan horses, worms, and other programs designed to do similar damage, *see* NRC REPORT, *supra* note 5, at 65 n.20-21.

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).[78] In this view, the proper focus of the constitutional inquiry should not have been on the verbal qualities of computer source code, but on the activities regulated under the definition of "export" employed by ITAR.

ITAR defines prohibited export activities to include "disclosing (including oral of visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad."[79] Technical data, in turn, is defined to include "information . . . which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles."[80] Such a sweeping definition arguably reach virtually all information that could be remotely useful in constructing a defense article, and thus, to avoid striking the entire regulation as overbroad, the Ninth Circuit in *Edler*[81] adopted a narrow definition of "technical data" to include only the export of information "significantly and directly related to specific articles" on the Munitions List. However, this reading does not solve our present dilemma because activities like talking to someone who is a foreign national about cryptography, teaching a class with international students about cryptography, placing an assignment on cryptography on a public Internet site all seem to be prohibited, insofar as they relate directly to cryptography — a defense article.[82]

With this wide broom, ITAR sweeps under all manner of activities which have been traditionally considered speech[83] and does so in a content-based manner, because the regulation's prohibitions are triggered only when the activities relate to cryptography, but not other types of algorithms or software.[84] The cryptographic provision in ITAR is aimed

---

78. *See* TRIBE, *supra* note 69, § 12-7, at 831 (arguing that even non-verbal acts can acquire an expressive dimension when the overall activity is viewed in a social context).

79. 22 C.F.R, § 120.17 (a)(4) (1996).

80. *Id.* at § 120.10(a)(1).

81. United States v. Edler, 579 F.2d 516 (9th Cir. 1978).

82. For a more extensive list of activities and analysis of their treatment under ITAR, see Laura M. Pilkington, *First and Fifth Amendment Challenges to Export Controls on Encryption:* Bernstein *and* Karn, 37 SANTA CLARA L. REV. 159, 183 (1996).

83. *See* TRIBE, *supra* note 69, § 12-7, at 829 (arguing that certain activities are historically and inextricably linked with speech).

84. *Cf.* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976) (invalidating a statute which prohibited advertising drug prices to prevent price competition because the aim of the statute was to suppress information); Linmark Assocs., Inc. v. Township of Willingboro, 431 U.S. 85 (1977) (striking down an ordinance prohibiting the placement of "For Sale" and "Sold" signs — in order to prevent white flight from certain neighborhoods — as content-based prohibition of speech).

at suppressing the dissemination of information and ideas, widespread knowledge of which the government considers to be *per se* dangerous.[85] It is this content-specific restriction on speech, rather than some intrinsic quality of software itself, that implicates the First Amendment's protection in its strongest form.[86] Thus, the court was correct to conclude that the appropriate standard of analysis is not the relatively lenient test of *United States v. O'Brien*,[87] but the much more stringent standards enunciated in *New York Times Co. v. United States*.[88] However, it need not have struggled through a largely incoherent exploration of the linguistic qualities of high-level source code, nor need it have gone so far as to find a general protected speech interest in all computer software.

B. What is "Export"?

Even if ITAR survives the foregoing analysis, it could have been invalidated for unconstitutional vagueness. A regulation is usually considered unconstitutional when persons of "common intelligence must necessarily guess at its meaning and differ as to its application."[89] The First Amendment's requirement of specificity stems from a concern for the "chilling effects" on speech of a vague standard.[90]

The export control regime over cryptography is the very paradigm of vagueness. For example, would placing cryptographic information on an Internet site for students qualify as "export" and subject the teacher to criminal sanctions under ITAR because foreigners may access the site?[91] Not only is a person of "common intelligence" unable to answer

---

85. *See* TRIBE, *supra* note 69, § 12-2, at 789-92 (explaining that when a prohibition singles out "actions for government control or penalty . . . because of the effects produced by awareness of the information or ideas such actions impart" it triggers a more stringent test than when it aims at noncommunicative impact in a content-neutral way).

86. *See id.* at 831 n.40.

87. 391 U.S. 367, 377 (1968) (weighing such factors as whether the government has constitutional authority to regulate a particular subject, whether the regulation furthers substantial government interests, whether the interest is unrelated to suppression of speech, and whether the restriction on speech is minimal).

88. 403 U.S. 713, 730 (1971) (Stewart, J. and White, J., concurring) (concluding that prior restraint of the speech, in its purest form, is only justified when disclosure would "result in direct, immediate, and irreparable" harm).

89. Connally v. General Constr. Co., 269 U.S. 385, 391 (1926).

90. *See* TRIBE, *supra* note 69, § 12-31, at 1034.

91. Consider Pretty Good Privacy ("PGP"), an cryptographic program designed by Philip Zimmermann, now one of the most widely used systems for secure e-mail. Originally, Zimmermann wrote the program as "freeware" and gave it to another party, who posted PGP on a USENET newsgroup. Zimmermann was careful to state that PGP was not for export, but it was quickly downloaded by sites throughout the world. The Justice Department closed its criminal investigation of Zimmermann in 1996 without filing charges.

this one, but the National Research Council's own committee to study cryptography concluded after an exhaustive survey of government-issued opinions that "the issue remains murky."[92] Cryptologists, who view the Internet as a natural and promising vehicle to collaborate and conduct research on cryptography, were equally baffled about what was permitted. Yet the *Bernstein* court glosses over this critical problem by declaring: "It seems reasonably clear that uploading an item to an Internet site that can be accessed in a foreign country constitutes 'sending' a defense article out of the country."[93] It went on to declare on that basis that "export" under ITAR is not unconstitutionally vague.[94]

An example of how easy it is inadvertently to violate the export laws in the Internet environment will illustrate the problem. The National Institute of Standards and Technology placed a publication containing source code for part of the Data Encryption Standard on its Internet site without an export restriction notice. The files were immediately copied by computers in Denmark, the UK, and Taiwan. The institute soon realized its violation of ITAR and moved the files, but the source code is now "available from hosts throughout the world along with the notice that export from the U.S. is in violation of U.S. export control."[95]

It is almost impossible on the Internet to determine whether one is communicating with a site within the United States or abroad at any given moment because there is no logical connection between someone's Internet Protocol (IP) address and that person's geographical location.[96] In this sense, the Internet is everywhere and nowhere at once, and there are zero costs in moving across international borders.[97] There are no visual clues or reminders that one has left the U.S. when visiting foreign

---

See NRC REPORT, *supra* note 5, at 164. During the fall of the Soviet Union, Zimmermann received email from Latvia, saying, "If dictatorship takes over Russia . . . your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks." William M. Bulkeley, *Cipher Probe: Popularity Overseas of Encryption Code Has the US Worried*, WALL ST. J., Apr. 28, 1994, at 1.

92. NRC REPORT, *supra* note 5, at 142-43 (noting that there is only one existing opinion from the ODTC, which specifies that under certain circumstances cryptographic software may be placed on the Internet if, among other things, "the software is placed in a file or directory whose name changes every *few minutes*") (emphasis added).

93. Bernstein v. United States Dept. of State, 945 F. Supp. 1279, 1294 (N.D. Cal. 1996).

94. *Id.*

95. Stephen Walker, *Testimony Before the Committee on the Judiciary Subcommittee on Technology and the Law of the United States Senate*, *in* BUILDING IN BIG BROTHER: THE CRYPTOGRAPHIC POLICY DEBATE 477, 482 (Lance J. Hoffman, ed., 1994).

96. David R. Johnson and David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996).

97. *See* Sean P. Kanuck, Recent Development, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 272 (1996).

sites on the Internet.[98] Similarly, there are few barriers to foreign Internet users from accessing U.S.-based sites. Thus, the only way to cure the vagueness of the regulation is to conclude that placing *any* cryptographic information on an Internet-accessible site is a violation of ITAR.

A similar problem arises with other activities such as teaching or presenting a paper at a conference.[99] The only way to be certain that one is complying with the law is to obtain a ruling from the ODTC, a process that is as cumbersome as it is unpredictable. Bernstein himself represents a case in point. The first ruling was so vague as to leave him uncertain whether his academic papers were covered; the second determined that *everything* was covered under the Munitions List; and a third disavowed the earlier opinion and maintained that only the source codes were covered.[100] As Judge Patel noted, "It is disquieting that an item defendants now contend could not be subject to regulation was apparently categorized as a defense article and subject to licensing for nearly two years."[101] Because individual researchers are often left unsure whether they may publicly discuss their cryptography research, the "chilling effect" of the regulation is substantial.[102]

As a result, export controls have far-reaching effects within the United States itself that can inhibit academic research and collaboration on cryptography.[103] In the long run, this may hinder research and development of cryptography in the United States and may undermine the competitiveness of the U.S. cryptographic industry as compared with its foreign counterparts.[104] Of course, this "Cryptography Gap" may be

---

98. *See* Johnson & Post, *supra* note 96, at 1395.

99. *See* Kenneth J. Pierce, *Public Cryptography, Arms Export Controls and the First Amendment: A Need for Legislation*, 17 CORNELL INT'L L.J. 197, 202-04 (1984). (discussing the NSA's role in suppressing public discussion of cryptography); *see also* Judith Beth Prowda, *A Lawyer's Ramble Down the Information Superhighway: Privacy and Security of Data*, 64 FORDHAM L. REV. 738, 764 n.446 (noting harassment of travelers who carry cryptographic equipment, even with an "export" license).

100. Bernstein v. United States Dept. of State, 945 F. Supp 1426, 1435 (N.D. Cal. 1996).

101. *Id.* It appears that even the judge lost patience with the government's equivocation. *See id.* at 1434 n.12.

102. *See* Baggett v. Bullitt, 377 U.S. 360, 372 (1964) (noting that the primary danger from vague laws is their over-deterrence effect on those who seek to avoid risks of liability "only by restricting their conduct to that which is unquestionably safe").

103. *See* NRC REPORT, *supra* note 5, at 124 n.11.

104. *See id.* at 138-39 (noting that rationales for rejecting export licenses are not revealed to applicants, with the result that "an atmosphere of considerable uncertainty pervades the development process."); *see also* Charles L. Evans, *U.S. Export Controls 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 (1994); Mark B. Hartzler, *National Security Export Control on Data Encryption — How*

just as harmful to national security and law enforcement interests as the proliferation of cryptography abroad.[105]

V. CONCLUSION

While the *Bernstein* decision sets an important precedent in extending the protections of the First Amendment to software and source code, it leaves many important issues unclear. The court's reasoning, based on standard doctrinal assumptions, fails when viewed more closely in light of the technical realities of computer software and modern communications technologies. The court's ruling should be an invitation for the legislature and the public to participate in this debate, which may have far-reaching consequences for U.S. security. However, it is important to reframe many of these questions to take into account ambiguities created by the technologies themselves, such as what words like "speech" and "export" mean in the information society. By taking into account the conceptual challenges that the emerging technology presents, we will be in a better position to find coherent solutions and to strike a more rational balance between competing conceptions of security.

They Limit U.S. Competitiveness, 29 TEX. INT'L L.J. 438 (1994).

105. *See* NRC Report, *supra* note 5, at 166. The NRC Report argues that even senior national security officials concede that the widespread availability of cryptography abroad is an inevitability and that U.S. export controls can only buy time for law enforcement and national security agencies to adapt to the new information environment. *See id.* at 114. As cryptographic technology increases in sophistication and prevalence, and acts of computer crime and espionage increase, national security and law enforcement objectives converge with the interests of American citizens and businesses in developing effective cryptography to promote secure communication. *See id.* at 298-303. Thus, despite the polarized terms of the current debate, gradual relaxation of cryptographic export controls may ultimately be in the best interests of all *parties*. *See id.* at 300-39.