First Amendment Freedoms and the Encryption Export Battle: Deciphering the Importance of Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999)

David McClure
University of Nebraska College of Law

Follow this and additional works at: https://digitalcommons.unl.edu/nlr

Recommended Citation
David McClure, First Amendment Freedoms and the Encryption Export Battle: Deciphering the Importance of Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999), 79 Neb. L. Rev. (2000)
Available at: https://digitalcommons.unl.edu/nlr/vol79/iss2/6

This Article is brought to you for free and open access by the Law, College of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Nebraska Law Review by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.
First Amendment Freedoms and the Encryption Export Battle: Deciphering the Importance of Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999)

"Encryption technologies are the most important technological breakthrough in the last one thousand years. No other technological discovery ... will have a more significant impact on social and political life. Cryptography will change everything."1

TABLE OF CONTENTS

I. Introduction: Where Encryption Meets the First Amendment ........................................ 465
II. Encryption and Its Importance Today ........................................ 466
   A. Modern Encryption At Work ........................................... 467
   B. Encryption Regulations .................................................. 469
III. Bernstein v. United States Department of Justice ........................................ 470
IV. The Battle and the First Amendment's Effect on It ........................................ 472
   A. The Battle Lines ......................................................... 472
   B. Which Side Should the First Amendment Favor? .................. 477
   C. Future Implications ...................................................... 482
V. Conclusion: The Greater Importance of Bernstein ........................................ 483

I. INTRODUCTION: WHERE ENCRYPTION MEETS THE FIRST AMENDMENT

For many years, a battle has raged over export restrictions on strong encryption products. Encryption ensures confidential and se-
cure communications among individuals, and the Commerce Depart-
ment and the State Department have long restricted its export
because of national security concerns. Industry and privacy groups
have fought against the restrictions for various reasons, ranging from
the desire to sell encryption software in new markets to preventing
government from accessing personal communications between indi-
viduals. Daniel Bernstein, a computer science graduate student,
challenged these restrictions in 1996, placing himself in the center of
this ongoing battle. In 1999, the Ninth Circuit Court of Appeals held
in Bernstein's favor, saying that such restrictions constituted a viola-
tion of the First Amendment. This ruling changed the dynamic of the
encryption export debate, and it has helped propel to victory those
who oppose regulations on the technology.

The first part of this casenote provides background information
necessary to understand the history and nature of encryption technol-
ogy and the regulations that restrict its export. The second part pro-
vides a detailed analysis of Bernstein v. United States Department of
Justice. The casenote ends with an examination of the competing
views in the encryption export battle and a discussion of the First
Amendment's influential role in the overall conflict.

II. ENCRYPTION AND ITS IMPORTANCE TODAY

Cryptography, the art of secret writing, has existed in some form
since the dawn of history — from the first observers of Egyptian hier-
oglyphs to the biblical Daniel's deciphering of handwriting on the
wall. It has been a passion and practice of some of history's notable
figures, including Thomas Jefferson who is considered the "Father of
American Cryptography" for his invention of the "wheel cypher" in the
1790s. Throughout the ages, cryptography's most visible partici-
pants have been governments and militaries fighting battles and wars
in which intercepted and deciphered messages meant victory or de-
feat. Approximately thirty years ago, however, cryptography started taking on greater importance outside the realm of kings and spies.

2. See infra notes 29-37 and accompanying text.
3. See infra notes 63-70 and accompanying text.
4. See Bernstein v. United States Dep't of Justice, 176 F.3d 1132, 1136 (9th Cir.
1999).
5. See id. at 1145.
6. 176 F.3d 1132 (9th Cir. 1999).
8. See id. at 80; Daniel 5:5-29.
9. See KAHN, supra note 7, at 192-195.
10. See WALTER B. WRISTON, THE TWILIGHT OF SOVEREIGNTY: HOW THE INFORMATION
Modern encryption emerged during the 1970s as a result of government and industry research and interaction — the primary players being Stanford and MIT researchers, IBM, and the National Security Agency.\(^\text{11}\) This research produced two important breakthroughs in cryptosystems: (1) the Data Encryption Standard (DES); and (2) RSA (the Rivest-Shamir-Aldeman algorithm).\(^\text{12}\) These new technologies, combined with the advent of other modern communication technologies, such as the fax machine and internet, were major steps in encryption’s expansion beyond governmental and military usage.\(^\text{13}\) The efforts of software engineer Philip Zimmerman took the process even further. He developed Pretty Good Privacy (PGP), encryption software for ordinary e-mail, and published it as freeware in 1991.\(^\text{14}\) This made encryption available worldwide and greatly concerned the United States government, prompting it to initiate a three-year criminal investigation of Zimmerman based on U.S. export restrictions.\(^\text{15}\) While worldwide security for sending messages would seem to be a positive development, such protection worried officials concerned with national security. In order to understand these governmental fears, it is important to recognize how modern encryption works.

A. Modern Encryption at Work

Modern digital encryption has been described as a “lockbox” placed around a message by the sending party that can only be retrieved by someone with the appropriate electronic key.\(^\text{16}\) The value of the technology is its ability to maintain the secrecy and security of the message throughout the delivery process. One commentator states:

The technology is the equivalent of the lock on the front door of a house. Without a lock, the house would have limited value and would be difficult to sell. With a relatively low-cost lock in place, the contents of the house are secure, and the value of the house increases tremendously.\(^\text{17}\)

This is the general function of encryption, but it is necessary to examine more technical aspects and terminology\(^\text{18}\) to understand where governmental anxieties originate. One scholar provides this


\(^{12}\) See id.

\(^{13}\) See Bernstein v. United States Dept’ of Justice, 176 F.3d 1132, 1137 (9th Cir. 1999).

\(^{14}\) For more information on Phil Zimmerman, see his website (visited Sept. 8, 2000) <http://www.pgp.com/phil/>.

\(^{15}\) See id.

\(^{16}\) See Bernstein, 176 F.3d at 1148 (Bright, J., dissenting).


\(^{18}\) For a glossary of encryption terminology, see Bert-Jaap Koops, The Crypto Controversy: A Key Conflict in the Information Society 269-70 (1999); Center
concise explanation of the encryption process: "using a computer program, an encryption algorithm (a mathematical equation) converts a plaintext message and encodes it, using a key, into apparently unintelligible ciphertext." Each component is critical to the process, but it is the electronic key that is at the center of the encryption controversy. Keys are used to encrypt and decrypt messages. There are primarily two types of encryption systems: 1) private key systems, also known as "secret key," "single key," or "symmetric" key systems; 2) public key systems, also known as "public-private key," "dual key," or "asymmetric" key systems. In private key systems, both the sender and receiver use the same key. In public key systems, two keys are used — a public key that is posted on the internet or elsewhere that can only be used to encrypt the message, and a private key that is held by the recipient party solely to decode the message. Public key systems are more advantageous in that they avoid the danger of transporting the same key between parties.

In each of the two systems, keys consist of "bits," which are the binary units of information that have the value 0 or 1. In order to decode a message by "brute force" (i.e., without having the key), it is necessary to try every possible key combination. Therefore, the longer the key, the more difficult it is to decipher the message. The strength of the encryption key grows exponentially with each additional bit. For example, a one-bit key would have two possibilities, but a two-bit key would have four possibilities. The Digital Encryption Standard (DES), the standard since the 1970s, uses a 56-bit key, and thus has $2^{56}$ possibilities (or approximately $7.2057594 \times 10^{16}$ possibilities). Philip Zimmerman's PGP troubled government officials because it used a 128-bit key. It is possible to crack a 56-bit key using a number of high-powered computers, but current technology would take several trillion times the age of the universe to crack a
128-bit key. Uncrackable encryption technology in the hands of terrorists, drug smugglers, tax evaders, and foreign governments could frustrate U.S. law enforcement and foreign policy interests.

B. Encryption Regulations

Despite its possible illegal uses, encryption is not regulated in any manner within the United States; individuals can sell, manufacture, use, and import encryption technology of any strength. There are restrictions, however, on the export of strong encryption technology. Such restrictions are not a new development, but opposition to them has reached fever pitch in recent years. The Arms Export Control Act (AECA) and the Export Administration Act (EAA) govern the export of encryption. Prior to 1996, the State Department was charged with promulgating International Traffic in Arms Regulations (ITAR) to implement AECA. Under these regulations, encryption software was frequently designated as a "munition" and placed on the United States Munition List (USML) pursuant to ITAR. In 1996, President Clinton issued an Executive Order transferring jurisdiction over nonmilitary encryption products from the State Department to the Department of Commerce. The Executive Order mandated that nonmilitary encryption products that normally would be placed on the USML would instead be moved to the Commerce Control List (CCL) under the Commerce Department-administered Export Administration Regulations (EAR). Encryption products designed solely for military purposes remained on the USML and under ITAR. Under both ITAR and EAR, individuals must obtain a license prior to exporting certain types of encryption technology. It was in this context that Daniel Bernstein and the First Amendment took center stage.

27. See Soma & Henderson, supra note 11, at 127.
29. See Joe Salkowski, Encryption Campaign Ends with a Triumph for Common Sense, Chi. TIm., Sept. 27, 1999, at 6 ("Government restrictions on encryption date back to the days of the earliest computers, which were used to decode military messages during World War II.").
37. 15 C.F.R. §734.2 (1999). For detailed background information on the encryption regulations, see Bernstein v. United States Dep't of Justice, 974 F. Supp. 1288 (N.D. Cal. 1997) and Saunders, supra note 19. The author is indebted to these sources for their statutory citations and understanding of the regulations.
III. BERNSTEIN V. UNITED STATES DEPARTMENT OF JUSTICE

Bernstein ran into the encryption export restrictions in 1992. As a graduate student at the University of California at Berkeley, he developed "Snuffle," a zero-delay private-key encryption system. The expression of his encryption system took three different forms: (1) a paper with Bernstein's analysis and math equations; (2) two computer programs written in "C"—his source code; (3) instructions in English, which were basically a translation of his source code into prose form. Bernstein wanted to present his work within academic and scientific communities worldwide. He submitted a commodity jurisdiction request to the State Department to determine whether his work fell under ITAR. The State Department responded affirmatively, saying that because his program was a munition under ITAR, he would need a license to export the paper, source code, or instructions. A series of contentious exchanges through the mail ensued between Bernstein and the State Department. When this failed to produce an agreement, Bernstein filed suit in 1996 to challenge the constitutionality of the ITAR regulations.

In the initial case of Bernstein v. United States Dep't of Justice, the district court held that source code was speech for First Amendment purposes; thus, Bernstein's claim was justiciable. In the second hearing of Bernstein v. United States Dep't of Justice, the district court ruled that particular ITAR provisions were unconstitutional under the First Amendment as prior restraints on speech. The court then extended its rationale of Bernstein II to the new EAR regulations under the Commerce Department in the third case of Bernstein v. United States Dep't of Justice. The appeal of Bernstein III resulted in the Ninth Circuit opinion that is the subject of this casenote.

A three judge panel from the Ninth Circuit reviewed Bernstein's case, and Judge Fletcher provided the Court's official opinion. The court affirmed the lower court's holding in Bernstein III that certain Commerce Department EAR regulations violated the First Amendment and enjoined enforcement of the particular regulations. In its analysis, the court began by examining a brief history of cryptography and noted that "[t]he interception and deciphering of foreign communications has long played an important part in our nation's national

40. 945 F. Supp. 1279 (N.D. Cal. 1996) ("Bernstein II").
42. See Bernstein, 176 F.3d at 1147.
security efforts."

The court then discussed pertinent portions of the EAR regulations, particularly focusing on how the definition of "export" was broader for encryption software than for other products under the EAR. For example, "export" for encryption included publication via internet, CD-ROM, and floppy disks, even though source code printed on paper was not subject to the regulations.

Following its discussion of history and the regulations, the court discussed the First Amendment doctrine of prior restraint. Judge Fletcher emphasized the special reverence accorded the First Amendment and the suspicion that arises with prior restraints on speech in licensing schemes, such as the EAR. As part of his prior restraint analysis, Judge Fletcher had to determine whether the regulations bore "a close enough nexus to expression." The government argued that encryption source code was not sufficiently related to expression because of its functional ability to control a computer. Nonetheless, Judge Fletcher rejected this argument and found that source code was expressive for First Amendment purposes; furthermore, he found that such code was not capable of controlling a computer.

The court asserted that source code served the same expressive function for programmers as equations do for mathematicians or graphs do for economists. It also noted how, in this particular case, Bernstein specifically used his source code as a means to speak out against the current regulations — in other words, "political expression." The court concluded by stressing the narrowness of its opinion in so far as it applied only to source code and not to all software products, and ended with dicta suggesting that regulations on encryption may endanger other fundamental rights beyond the First Amendment.

Judge Bright's concurrence placed him squarely between Judge Fletcher's opinion and the dissent. Judge Bright acknowledged that source code has both communicative purposes as expression as well as functional purposes for controlling computers. His concurrence declined to resolve the issue; rather, Judge Bright suggested that the United States Supreme Court review the matter.

Judge Nelson's dissent viewed computer source code as an inherently functional device that is more like conduct than speech. In his view, because source code is conduct, the regulations were valid and

43. Id. at 1137.
44. See id. at 1137-38 (citing 15 C.F.R. §§ 734.2(b)(9)(B)(ii), § 734.3(b)).
45. See infra note 87.
46. See Bernstein, 176 F.3d at 1139.
47. Id.
48. See id. at 1142.
49. See id. at 1141.
50. Id. at 1141 n.14.
51. See id. at 1145-46.
should be enforced. He acknowledged that programmers may occasionally use source code as a communication device, but he maintained that such use is rare. Judge Nelson concluded by stating that Bernstein may indeed have an "as-applied" First Amendment claim, but not a facial challenge to the regulations.52

On September 30, 1999, the Ninth Circuit voted to withdraw the three-judge panel opinion and rehear Bernstein's case by the en banc court.53 On April 11, 2000, the court decided to remand the case to the district court in light of the new encryption export regulations adopted on January 14, 2000.54 While the opinion discussed above is no longer the law, it is still an important case because of its influence on the larger encryption export battle. It provides insight into the competing interests and issues at stake in the debate. These issues and the role the First Amendment has played in determining the battle's outcome are the subjects of the next section.

IV. THE BATTLE AND THE FIRST AMENDMENT'S EFFECT ON IT

A. The Battle Lines

To fully understand the importance of Bernstein, it is necessary to explore further the present state of the encryption export battle. Three general positions in the war have emerged: (1) those who are in favor of restrictions on encryption exports; (2) those who oppose any such restrictions; (3) those who are in the middle (i.e., individuals in favor of some restrictions, but who believe encryption should be unregulated for the most part).55 By examining these groups and recent trends in the debate, it is possible to see what effect the First Amendment analysis and result in Bernstein have had on the ultimate outcome of the encryption export battle.

The proponents of restrictions are primarily the government, law enforcement agencies, militaries, and those who see encryption as a threat to national security. These entities and individuals strongly support export restrictions on encryption. Some even support forms of domestic regulation, such as requiring individuals to automatically make a copy of their encryption key for deposit with the government

52. See id. at 1149 (dissenting opinion).
53. See Bernstein v. United States Dep't of Justice, 1999 WL 782073 (9th Cir.).
54. See Electronic Frontier Foundation, 9th Circuit decision to dismiss appeal and remand back to district court (Apr. 11, 2000), (last visited Sept. 8, 2000) <http://www.eff.org/bernstein/Legal/20000411_remand_order.html>.
55. See, e.g., Educom Review Staff, Encryption Technology & Crime: Searching for a Neutral Zone, 32 Educom Rev. 5 (last visited Sept. 8, 2000) <http://www.educause.edu/pub/er/review/reviewArticles/32538.html> (interviewing Dorothy Denning, who believes regulations should allow for government access, but only under tightly controlled circumstances).
or a designated third party (a process known as "key escrow" or "key recovery"). Governments and militaries worry that unlimited access to strong encryption will give foreign governments and individuals the tools for "information warfare" — the "purposeful and strategic use of information, the ability to cripple a country by decrypting its coded messages, seizing its financial centers, and disabling its communication hubs." More importantly, foreign governments with strong encryption are not as susceptible to U.S. attempts to intercept and decode their communications. As one scholar notes, "Though the technology has changed dramatically, the intent has remained the same: to read the enemy's messages and to keep one's own secret." On the other hand, some have suggested the U.S. government continue its consistent support of restrictions in order to preserve good relations with other countries, such as France, which maintain very strict controls on encryption.

Law enforcement officials, such as U.S. Attorney General Janet Reno and FBI Director Louis Freeh, additionally fear that strong encryption will increase the amount of crime, as criminals utilize encryption to conceal illegal activities. Freeh, one of the most outspoken figures in favor of restrictions, testified that "the widespread availability and use of robust, non-recoverable encryption ultimately will devastate our ability to fight crime and prevent terrorism." Drug smugglers, terrorists, distributors of pornography, and gambling ring-leaders are classes of criminals that may come to mind as likely encryption-users, but tax-evaders and money-launderers will also enjoy protection in the new world of on-line transactions and money in

---


57. Id. at 765.

58. WRISTON, supra note 10, at 154.


61. See, e.g., Klopfenstein, supra note 56, at 772 n.55 (listing congressional committee hearings that discussed encryption use by Cali Cartel, other violent criminals, and a gambling ring).
the form of "digital blips." Thus, from the FBI to the IRS, government officials hope encryption restrictions will enable them to track criminals and build sufficient cases to convict them.

The contrary view regarding encryption decries any regulations on the export or use of the technology. Industry, privacy groups, academics, and those who view government encryption regulations as an intrusion by a "Big Brother" government share this perspective. Regardless of the subgroup, the same argument surfaces continually: "Anyone who wants strong encryption can already get it." Industry uses the argument to bolster its position that it is being denied access to a multi-billion dollar market from which businesses in other countries are reaping the benefits. U.S. businesses point to the desirability of security in e-commerce and the potential for even greater consumer confidence in on-line transactions. These businesses believe market forces should determine whether key escrow is necessary and argue that strong encryption actually decreases crime. Furthermore, they point to industry's already successful attempts to circumvent the restrictions by establishing foreign subsidiaries to sell the encryption technology overseas.

Privacy groups, such as the Electronic Frontier Foundation and the Center for Democracy and Technology, use the argument to support their contention that restrictions unnecessarily burden scientific expression, hinder human rights in other countries, and endanger individual privacy interests from government intrusion. Additionally, those who specialize in encryption argue that encryption possesses two unique features that are not conducive to regulation: (1) dissemination of the technology is necessary in order to allow others the opportunity to crack the system and find weaknesses in the program; (2) any openings in the program, such as key escrow, provide additional possibilities for a security breach, and thus inherently weaken the program. Others argue that the restrictions are simply outdated—they may have worked when an encryption system was a "room-size collection of vacuum tubes and switches," but they do not make sense in a world where the software can be "e-mailed around the world in the time it takes a customs inspector to uncap his pen." Finally, this group heralds the tremendous potential for good from the technology,

63. Salkowski, supra note 29, at 6.
65. See Klopfenstein, supra note 56, at 789.
66. See Cockburn, supra note 64, at 507.
67. See Koops, supra note 18, at 54-55.
68. See Klopfenstein, supra note 56, at 777, 789.
69. Salkowski, supra note 29, at 6.
from creating digital signatures to securing the privacy of vitally important communications. They believe encryption regulations do not prevent criminal activity, but instead serve only to keep the strongest encryption out of the hands of those who need it most.\textsuperscript{70}

The final perspective on encryption falls between the two ends of the spectrum. This group of “middle-grounders” supports some regulation on encryption but primarily favors freedom from regulation. These individuals have not given up on governmental regulation as an effective tool to protect national security, and they are willing to sacrifice some privacy for that purpose. Dorothy Denning, a computer science professor, articulated this middle-ground view. She stated, “We have never really had absolute privacy with our records or our electronic communications — government agencies have always been able to gain access with appropriate court orders.”\textsuperscript{71} The problem with this viewpoint is that regulation which truly balances privacy interests with government interests results in insufficient protection of national security,\textsuperscript{72} and there is some doubt as to whether such tailored and balanced regulations can provide any protection at all.

Recent developments favor those who oppose regulations on encryption software. Since the inception of the encryption battle, Congress has proposed legislation to deal with the issue; however, few bills have gained the approval of both Congress and the President. What can be said regarding the proposals is that, even in the most restrictive bills, there appears to be a trend toward liberalizing the export restrictions. Two proposals in the 106th Congress dealing with the export regulations are the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999\textsuperscript{73} and the Security and Freedom through Encryption (SAFE) Act.\textsuperscript{74} The PROTECT Act was sponsored by Senator John McCain and is the more restrictive of the two bills. The bill seeks to establish an Encryption Export Advisory Board that would recommend exemptions to encryption technology “where similar, foreign produced products are generally, and publicly available, or where such foreign produced products will be in the marketplace within 12 months.”\textsuperscript{75} Thus, while the bill still seeks to restrict encryption, it recognizes the wide availability of encryption through foreign outlets. In fact, the Committee report states that “[t]he worldwide ubiquity of encryption makes the technology impossible to control.”\textsuperscript{76} The SAFE Act in the House provides an

\textsuperscript{70} See Koops, supra note 18, at 130-31.
\textsuperscript{71} Educom Review Staff, supra note 55.
\textsuperscript{72} See Klofenstein, supra note 56, at 806-07.
\textsuperscript{73} S. 798, 106th Cong. (1999).
\textsuperscript{74} H.R. 850, 106th Cong. (1999).
\textsuperscript{76} Id.
even more liberal approach to encryption software than the PROTECT Act. Both proposals exhibit the strong movement of the overall battle toward fewer restrictions on encryption exports.

The White House has also significantly tempered its support for strict encryption regulations. On September 16, 1999, the Clinton Administration announced plans to further liberalize its policy on encryption export restrictions. The new regulations, which took effect on January 14, 2000, allow publicly available encryption source code to be exported without review or classification, as long as the exporter submits written notification of the internet site or a copy of the source code to the Bureau of Export Administration. On July 17, 2000, the Clinton Administration announced even further updates to the export regulations. If adopted, these regulations would allow anyone to export without a license any encryption product to an individual or government entity in the European Union, Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand, and Switzerland.

The new revisions would also make it clear that publicly available source code and the object code that results from compiling it would receive the same treatment. Proponents for the free-flow of encryption software see the Clinton Administration’s actions as a sign of surrender to the realities of the easily-spread technology.

These changes in policy have placed anti-regulation advocates at the doorstep of victory in the export battle. In fact, the Commerce Department has given Daniel Bernstein permission to publish his source code on-line. However, Bernstein’s attorney contends that allowing publication on the internet while still retaining prohibitions against knowingly exporting code to states supportive of terrorism is “an area of ambiguity that remains.”

---

78. See 65 Fed. Reg. 2492 (2000). The regulations are codified at 15 C.F.R. Parts 734, 740, 742, 770, 772, and 774. Id.
79. Id. at 2493.
81. See id.
83. See Salkowski, supra note 29, at 6. But cf. A Switch on Encryption, supra note 60, at 806 (suspecting the Clinton Administration's announcement is based more on political considerations than national security concerns).
85. Id. The regulation at issue is codified at 15 C.F.R. § 740.13(e)(2) (2000) and lists Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria as supporters of terrorism.
cifically state that making source code available on the internet for anyone's use "would not establish 'knowledge' of a prohibited export," which appears to address Bernstein's question. Nonetheless, if there is an ambiguity, the district court's determination of Bernstein's First Amendment claim could serve an important role in resolving the dispute.

B. Which Side Should the First Amendment Favor?

Bernstein's challenge forced the First Amendment to take sides in the encryption export debate. The Bernstein court was faced with the task of determining whether source code was "speech" for purposes of First Amendment protection. The well-settled First Amendment test for symbolic speech established in United States v. O'Brien would seem to provide a clear solution for courts in making this determination. However, the unique attributes of encryption source code and the imprecise balancing of the O'Brien test have resulted in courts reaching disparate conclusions while searching for the perfect analogy to solve the constitutional question.

Encryption source code does not fall under the traditional First Amendment categories of the written or spoken word, since it can be both expressive and functional. However, the Supreme Court has consistently held that First Amendment protection can extend to certain types of conduct or "symbolic speech." The Court addressed the issue of symbolic conduct in United States v. O'Brien. In 1966, David Paul O'Brien and three others burned their Selective Service registration certificates on the steps of a courthouse in protest of the Vietnam War. A crowd witnessed the event and began to attack the men. O'Brien was later arrested and convicted of knowingly destroying his draft card, a federal offense. He argued that the law under which he was charged was an unconstitutional abridgement of

87. The Bernstein court approached the broader issue of whether the government's licensing scheme constituted a prior restraint of speech, which required it to "determine whether encryption source code [was] expression for First Amendment purposes." Bernstein, 176 F.3d at 1139. The court's determination of this sub-issue is the focus of this casenote, and the broader issues of prior restraint and government licensing are beyond the scope of this inquiry.
89. See Junger v. Daley, 209 F.3d 481, 484 (6th Cir. 2000).
92. See id. at 369-70.
93. See id. at 369.
94. See id. at 369-70.
The Supreme Court refused to endorse the view that all activities with some expressive purpose are "speech" under the First Amendment; rather, they acknowledged that "a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." The Court introduced a four-part test to determine whether a regulation that restricts symbolic speech is justified:

[W]e think it clear that a government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

The O'Brien court determined that the statute's purpose to insure the smooth functioning of the Selective Service System was a substantial governmental interest unrelated to suppressing free speech and in line with Congress' power to raise armies.

Only three cases have addressed the issue of encryption source code's expressive value in relation to the government's export restrictions — Bernstein, Karn v. United States Dep't of State, and Junger v. Daley. The cases have similar fact patterns, but each court has approached the issue in a different way, which highlights the difficulty of applying O'Brien principles to a complex technological issue. The first part of the O'Brien test that requires the regulation to fall within the government's constitutional power has not been challenged in any of the encryption cases. Likewise, O'Brien's second requirement of a substantial governmental interest has not raised significant objections because national security, foreign policy, and national defense are legitimately important interests.

Divergence among the courts occurs in the third and fourth parts of the O'Brien test. O'Brien's third requirement forces courts to decide whether the government's interest in national security is related to

95. See id. at 370.
96. See id. at 376; accord Dallas v. Stanglin, 490 U.S. 19, 25 (1989) (stating that "[it is] possible to find some kernel of expression in almost every activity a person undertakes — for example, walking down the street or meeting one's friends at a shopping mall — but such a kernel is not sufficient to bring the activity within the protection of the First Amendment.").
98. Id. at 377.
99. See id. at 382.
100. 176 F.3d 1132 (9th Cir. 1999), reh'g granted and opinion withdrawn, 192 F.3d 1308 (9th Cir. 1999).
the suppression of free speech when the government regulates the export of encryption source code.105 Courts cannot decide this issue without first determining whether free speech is implicated in the case before them, and specifically, whether encryption source code is "speech." In their attempts to answer these questions, courts have scoured the archives of First Amendment cases in search of appropriate analogies to encryption source code that will dictate the right result.

The use of O'Brien has prompted courts to make the comparison or distinction between the writing of encryption source code and the burning of a flag or draft card in protest.106 The Bernstein court stretched the analogy of protest when it characterized Bernstein's attempt to end-run the encryption regulations as "political expression."107 Both Bernstein and the latest Junger case analogized computer scientist's expressive uses of source code to similar mathematicians' and economists' uses of equations or graphs.108 However, the initial Junger case concluded that such analogies overemphasized the expressive uses of source code and did not capture the essence of source code's functionality.109 The court stated, "Unlike instructions, a manual, or a recipe, source code actually performs the function it describes."110 The Sixth Circuit disagreed with the district court's choice of these analogies and reversed the decision.111 The court chose instead to utilize the Supreme Court's declaration that the "artwork of Jackson Pollack, the music of Arnold Schoenberg, or the Jabberwocky verse of Lewis Carroll" is "unquestionably shielded" by the First Amendment.112 The comparison of encryption source code to a musical score had particular appeal to the court because, like encryption, "a musical score cannot be read by the majority of the public but can be used as a means of communication among musicians."113

Each of the analogies utilized by the courts appears to make a logical connection to a strand in the bundle of attributes that makes encryption source code what it is. However, none of the comparisons accurately encapsulates the entire nature of source code. A computer scientist may wish to make a political statement by writing source

105. See O'Brien, 391 U.S. at 377.
108. See Junger, 209 F.3d at 484; Bernstein, 176 F.3d at 1141.
109. See Junger, 8 F. Supp. 2d at 717.
110. Id.
111. See Junger, 209 F.3d at 484.
112. Id. (citing Hurley v. Irish-American Gay, Lesbian and Bisexual Group, 515 U.S. 557, 569 (1995)).
113. Junger, 209 F.3d at 484.
code, but it is difficult to argue that the statement will be understood as easily as a protest on a courthouse steps during a time of war.\textsuperscript{114} Mathematical equations and graphs are the closest approximations to the appearance of source code and its potential for dangerous uses, but they are not quite identical to source code in their functionality (particularly graphs). The musical score analogy may be the best fit to encryption source code because a musical score facilitates music (protected speech) in a way similar to the manner in which encryption is used to facilitate communications among individuals (protected speech). However, the musical score analogy does not reflect the complexity of source code's potential connection to international terrorism and other foreign policy concerns, which may decrease its attractiveness to some courts. With a complex issue and such an array of awkward analogies for courts to choose, it should not be surprising that courts have not reached a consensus on whether source code is speech.

The fourth part of the \textit{O'Brien} test requires courts to determine if the incidental restriction on free expression is no greater than necessary to further the government's interest.\textsuperscript{115} This is a question of a regulation's tailoring, and the answer depends largely on the courts' conclusions to the prior parts of the \textit{O'Brien} test. In encryption cases, source code's relationship to object code also tends to further complicate a court's determination as to the extent of the government's interest. Programmers take source code, compile it, and transform it into object code, which is the series of 0's and 1's capable of running a computer (i.e., completely functional encryption software). The dichotomy between object code and source code is relevant in the technical computer sense, but for the purposes of export regulations, source code and object code can blur. The \textit{Bernstein} court expressly declined to address whether object code is expression under the First Amendment,\textsuperscript{116} but in practical terms, it might as well have. If source code is expression and is fully protected under the First Amendment, then restrictions on object code will not be very effective. Software for compiling source code is not universally compatible, but it is typically available.\textsuperscript{117} Foreign governments and individuals could receive unrestricted source code and easily compile it into object code. In this scenario, regulations would have practically no effect in stopping the flow of encryption technology overseas.

\textsuperscript{114} Compare encryption cases with \textit{Texas v. Johnson}, 491 U.S. 397, 406 (1989) (discussing how "the expressive, overtly political nature" of flag-burning at the Republican National Convention was "both intentional and overwhelmingly apparent") and \textit{Spence v. State of Washington}, 418 U.S. 405, 415 (1974) (stating that an American flag flown with an attached peace symbol as a reaction to the U.S. invasion of Cambodia was a "direct" and "likely to be understood" message).

\textsuperscript{115} \textit{See O'Brien}, 391 U.S. at 377.

\textsuperscript{116} \textit{See Bernstein}, 176 F.3d at 1141 n.15.

\textsuperscript{117} \textit{See Junger}, 209 F.3d at 483.
The Karn case also challenges the rational relationship between the government's interest and its means. Philip Karn submitted two commodity jurisdiction requests to the State Department for permission to export *Applied Cryptography*, a book that includes complete source code for strong encryption software and permission to export a computer disk containing verbatim copies of source code from *Applied Cryptography*. The State Department determined that the book did not fall under its jurisdiction under ITAR, but the diskette did and was classified as a munition. The court held that the regulations were content-neutral and should be upheld. Karn raises issues regarding the rationality of the government's restrictions on encryption. If foreign countries can obtain copies of books that contain source code for strong encryption technology, then one must wonder why computer disks and CD-ROMs are prohibited from export. Disks do make source code easier to manipulate and utilize, and books traditionally have strong First Amendment protection. Yet, this assertion lacks persuasiveness because foreigners will still have access to the critical information. The rationality of the regulations is further challenged by the lack of any domestic regulations on encryption. If one of the government's primary interests is in protecting the safety of its citizens from acts of terrorism or violence, that interest is not guarded from internal disturbances plotted over secure e-mail.

The arguments against classifying encryption source code as protected symbolic speech may have a slight edge in the search for the most appropriate analogy due to encryption's functionality and its lack of a clearly understood message, but the rationality of the export regulations is still an open question. The reversal of Junger has given encryption proponents a favorable 2-1 majority in encryption export cases, and the trend is likely to continue. Courts may tend to side with the holdings in Bernstein and Junger because of the possible expressive uses of source code, the fear of stifling a new technology, the seemingly irrational regulations, the recognition of an outside world where encryption technology is widely available, and the awareness that regulation is increasingly disfavored by Congress, the President, and large segments of American society. For better or for worse, the First Amendment has weighed in on the side of the encryption exporters, and in the case of Bernstein, it may have set events in motion to secure long-term victory for free speech allies, even if courts determine later that the First Amendment should not protect such activities.

---

118. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (1994).
119. See Karn, 925 F. Supp. at 10.
C. Future Implications

As the Bernstein case begins anew at the district court level, there are at least three possible implications of future Bernstein decisions. First, if the district court and Ninth Circuit continue to find that encryption export regulations offend the First Amendment, the victory march will continue for opponents of the regulations as the liberalizing trend gains momentum. This result would make it very difficult for both pro-regulation advocates and "middle-grounders" to impose even minimal restrictions on the export of encryption technology. Continued favorable rulings for anti-regulation forces would stifle attempts by government and others to regulate domestic encryption products, as well. If the courts consistently hold that source code is expression, they may open a door for First Amendment protection for other forms of software and code in the future.

The second possible scenario is that the courts will reverse course and find that encryption export regulations do not violate the First Amendment, allowing government to maintain a foothold in the area. Industry and privacy groups would need to consider alternative legal arguments, such as the Fourth Amendment, because law enforcement and government officials would be able to advocate even stronger encryption controls. Because the current export restrictions do not protect the U.S. from domestic criminals who have unlimited access to strong encryption, officials could reasonably target this group next. With the ability to regulate encryption, Congress and the President could continue to search for arrangements that strike a balance between national security and the interests of industry and privacy groups. A favorable result for the pro-regulation forces would also be a positive development for those in the middle that support minimal restrictions. However, even with a court victory in favor of restrictions, the mood of the country would need to shift significantly to halt the momentum of anti-regulation forces and to make more restrictive regulations feasible.

The third and final implication is the possibility that by the time the courts reach a consensus on this issue, the export regulations will be virtually non-existent or so easily bypassed that Bernstein will stand as a symbol of a bygone era. Industries have already found ways to export encryption in response to the market's demand for strong encryption both domestically and internationally. Demand

121. See Bernstein, 176 F.3d at 1146 ("Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, the right against compelled speech, and the right to informational privacy." (citations omitted)).
122. For a description of a foreign national taking advantage of available encryption during a stay in the U.S., see Mc Hugh, supra note 62.
123. See Cockburn, supra note 64, at 507.
for this technology will continue to increase as American and Canadian online retailers seek greater protection in an industry expected to generate $36.6 billion in 1999.124 New technologies are already available to bypass current restrictions. These innovative technologies, such as “chaffing and winnowing,”125 fall outside the encryption regulations, yet provide “encryption-like” security protection. There is even discussion of future encryption systems that will function according to the laws of quantum physics and “guarantee absolute security for eternity.”126 All sides must prepare for the possible consequences if technology does move beyond Bernstein and the First Amendment before the issue is resolved. This applies particularly to pro-regulation advocates, because they will not be able to rely comfortably on the efficacy of export restrictions even if the courts declare such restrictions constitutional.127

V. CONCLUSION: THE GREATER IMPORTANCE OF BERNSTEIN

Although Bernstein’s case is still in the court system, its legacy may already be established. The encryption export battle has moved steadily in favor of anti-regulation groups since Bernstein first started to challenge the system in 1992. The Bernstein decision in 1999 bolstered the anti-regulation cause and provided the Clinton Administration with a strong incentive to reevaluate its stance on encryption and

125. “Chaffing and winnowing” was proposed by Ronald Rivest in 1998. It involves breaking a message into packets (“good” packets, or “wheat”) and attaching an authentication code to each one. Similar packets are then created (“bad” packets, or “chaff”) and interspersed with the “good” packets. The recipient of the message uses the correct authentication key to separate the “wheat” from the “chaff.” Encryption is not involved in the process because the entire message is visible at all times. For a detailed explanation of “chaffing and winnowing,” see Saunders, supra note 19, at 953-57.
127. The Clinton Administration appears to recognize this problem. In the Cyberspace Electronic Security Act of 1999, the Administration planned to authorize $80 million for the FBI's Technical Support Center in an attempt to deal more effectively with encryption use by criminals. See White House Fact Sheet for Sept. 16, 1999, THE CYBERSPACE ELECTRONIC SECURITY ACT OF 1999 (visited Sept. 8, 2000), <http://www.pub.whitehouse.gov/uri-res/12R?urn:pid://oma.eop.gov.us/1999/9/16/16.text.1>. One possible method law enforcement officials may utilize is known as a “tempest attack,” which aims to detect the distinct electromagnetic signals emitted by a computer each time a letter is typed. If Eve parks a van outside Alice’s house, she can use sensitive tempest equipment to identify each individual keystroke that Alice makes on her computer. This would allow Eve to intercept the message as it is typed into the computer, before it is encrypted.

SINGH, supra note 126, at 318.
to modify the export regulations. Even if the Ninth Circuit reverses course now, the *Bernstein* decision has already helped set events in motion to secure long-term victory for the proponents of liberal encryption exports. That is not to say that subsequent decisions will not define future battles or determine the government's ability to regulate other emerging technologies, but in the case of encryption exports, those who wanted to export are now free to do so in most cases.

*Bernstein* and the encryption export debate are also significant because they reveal the intersection of important societal interests. Issues of this type force society to consider what interests it values most, and they issue a challenge to find ways to balance fundamental values of free speech and privacy with the critical interests of public safety, economic stability, and foreign policy. As technology further permeates the culture, issues that require such difficult weighing and balancing of values will continue to pose significant challenges for society in the new millennium.

*David McClure*