NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW AND COMMERCIAL REGULATION

Volume 24 | Number 1 Article 4

Fall 1998

Cryptobabble: How Encryption Export Disputes Are Shaping Free Speech for the New Millennium

Daniel R. Rua

Cryptobabble: How Encryption Export Disputes Are Shaping Free Speech for the New Millennium

Cover Page Footnote
International Law; Commercial Law; Law

COMMENT

Cryptobabble: How Encryption Export Disputes Are Shaping Free Speech for the New Millennium

> The exportation of encryption products must be controlled to . . . promote our national security, including the protection of the safety of U.S. citizens abroad.[1]
>
> —President William J. Clinton

> Only an emergency can justify repression. Such must be the rule if authority is to be reconciled with freedom. Such, in my opinion, is the command of the Constitution. It is therefore always open to Americans to challenge a law abridging free speech and assembly by showing that there was no emergency justifying it.[2]
>
> —Justice Louis Brandeis

---

[1] Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,573 (1996) (to be codified at 15 C.F.R. §§ 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772, 774) (announcing a plan to shift encryption export regulation control to the Department of Commerce).

[2] Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

I. Just Imagine

Although math is not traditionally a lawyer's forté, imagine discovering a new mathematical formula that, when applied correctly, would save thousands of lives and dollars across the world. Then imagine that the formula is so complex that the only hope of applying it correctly depends on computers doing the calculations. Therefore, to communicate your discovery to the world you create an electronic instruction manual written in computer language. Those skilled in computer languages may read the instruction manual to learn how your formula works. But, more importantly, the large majority of people in the world who are not as skilled may ask their computer to read it for them. In so doing, are those people reading an expression from you as the inventor and instruction manual creator? Is that an expression that deserves limited protection under Constitutional freedom of expression doctrines? What if users of the formula find a way to use it for bad purposes—is the original instruction manual any less of an expression?

The imaginary scenario and questions outlined above are currently being considered in federal courts,[3] on the Congressional floor,[4] and behind closed government doors.[5] The mathematical formula is one that allows people to scramble their computer files and their electronic communications in a way that is extremely difficult to unscramble.[6] This capability, termed "cryptography,"[7]

---

[3] *See infra* notes 129-272 and accompanying text.

[4] *See generally*, 143 CONG. REC. E2276 (daily ed. Nov. 9, 1997) (statement of Rep. Dreier supporting recent export regulations limiting encryption export); 143 CONG. REC. S10879 (daily ed. Oct. 21, 1997) (statement of Sen. Lott congratulating the House on recent progress toward encryption export reforms).

[5] *See* Charles L. Evans, Comment, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. INT'L L. & COM. REG. 469, 479 & n.130 (1994) (describing a phone interview with the National Institute of Standards and Technology, whereby the author was told the evaluation process for "encryption software is classified and not available to the public").

[6] *See infra* notes 55-70 and accompanying text.

[7] Cryptography, to most people, is concerned with keeping communications private. R.S.A. LABORATORIES, ANSWERS TO FREQUENTLY ASKED QUESTIONS ABOUT TODAY'S CRYPTOGRAPHY, VERSION 3.0, at 12 (1996) [hereinafter CRYPTOGRAPHY FAQ]. As uses for cryptographic algorithms have multiplied, however, the definition has been

is extremely valuable for corporations and individuals, but is also threatening to U.S. security agencies.[8] To understand these competing interests, it is important to recognize today's marketplace boundaries and how technology threatens security. This Comment examines both the benefits and the concerns with cryptography. It also considers how efforts to limit international export are focused on a means of expression, namely software, which is arguably equivalent to speech under the Constitution.

The Comment begins by detailing the evolution to this point in the encryption debate and provides a recent example highlighting inconsistencies in the present export scheme.[9] Part II of the Comment provides a foundation by defining the technology and terms involved, and by presenting the current regulations and process for encryption exporters.[10] Part III discusses the three cases that have reached the federal courts with regard to exporting cryptographic code.[11] The arguments from those cases are analyzed in Part IV which discusses the constitutional issues involved.[12] The most significant question presented by the cases is whether software is speech within the free expression protections that come with such a classification.[13] Part V focuses on the policy issues surrounding the encryption export dispute and how those issues shape regulations around the world.[14] Finally, Part VI discusses recent legislative proposals, along with guidance the Constitution and the courts have provided for refining those solutions.[15] That Part concludes by noting that such lessons not only impact contemporary export regulations, but also aid free

---

blurred. *See id.* At its base, "[c]ryptography today might be summed up as the study of techniques and applications that depend on the existence of difficult problems. A *cryptanalyst* attempts to compromise cryptographic mechanisms, and *cryptology* (from the Greek *kryptós lógos*, meaning 'hidden word') is the discipline of cryptography and cryptanalysis combined." *Id.*

[8] *See infra* notes 390-422 and accompanying text.

[9] *See infra* notes 17-54 and accompanying text.

[10] *See infra* notes 55-128 and accompanying text.

[11] *See infra* notes 129-272 and accompanying text.

[12] *See infra* notes 273-388 and accompanying text.

[13] *See infra* notes 281-95 and accompanying text.

[14] *See infra* notes 389-468 and accompanying text.

[15] *See infra* notes 469-85 and accompanying text.

expression interpretation as we move further into the information age.[16]

A. Internet Growing Pains

Ever since Vice President Albert Gore coined the term "Information Superhighway,"[17] the U.S. government has actively marketed the Internet[18] and its benefits with gusto.[19] President William J. Clinton has stated that "[t]he Internet should be a global free-trade zone."[20] The executive branch commissioned a report, "A Framework for Global Electronic Commerce,"[21] which aimed to create a uniform code for electronic commerce and to delegate many regulation issues to industry and consumer groups.[22] As a result of these efforts and the Internet's inherent attractions, businesses and consumers have flocked to the Internet.[23] In fact,

---

[16] *See infra* notes 468-81 and accompanying text.

[17] *See* 135 CONG. REC. S.1067, 9887 (daily ed. May 18, 1989) (statement of Sen. Albert Gore extolling the virtues of investing in high-speed networks to the nation).

[18] The Internet, while "surfed" by many to uncover interesting topics, is rather hidden to the casual user. Beneath its cohesive, marketed exterior, the Internet is "a conglomerate of hundreds of thousands of networks owned by government agencies, defense departments, universities, and corporations. Users can digitally discuss just about any specialized area of concern with other users, often with the leaders in their respective fields." Timothy B. Lennon, Comment, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467, 470 n.11 (1994).

[19] *See* Laura M. Pilkington, *First and Fifth Amendment Challenges to Export Controls on Encryption:* Bernstein *and* Karn, 37 SANTA CLARA L. REV. 159, 159 n.1 and accompanying text (1996) (noting that "[t]he federal government encourages the expansion of the Internet and hails it as a revolution in the dissemination of information and as an avenue for commerce").

[20] Ted Lewis, *We Don't Need No Regulation*, SCI. AM., Nov. 1997, at 1 (quoting President Clinton "in reversing his administration's stance on the export of encrypted computer products"). Although such remarks were hailed as an administration about-face and as an embrace of encryption, subsequent regulatory moves proved otherwise. *See infra* notes 108-09 and accompanying text.

[21] William J. Clinton, *Text of the President's Message to Internet Users* (visited Jan. 20, 1998) <http://www.whitehouse.gov/WH/New/Commerce/message.html> (announcing the release of a report outlining the administration's vision for the emerging electronic marketplace).

[22] *See* Lewis, *supra* note 20, at 1 (describing the report's general hands-off recommendation for many privacy, security, and commerce issues on the Internet).

[23] Internet size has doubled yearly since 1991. *See* Internet Facts (visited Nov. 20,

electronic communications have become the prominent means of communication for some circles.[24]

There are literally trillions of bits of information floating on the Internet involving various topics. This "digital information" includes law journal articles, financial records, medical records, electronic mail (email) messages, voice, video, and even pornographic pictures.[25] All of this digital information could be of interest to parties other than the transmitter and intended receiver. For example, oppressive governments may be interested in the email or voice communications of their citizens.[26] Less oppressive governments may also be interested in their citizens' communications if they suspect the content is illegal.[27] The most prevalent danger, however, is from hackers[28] who may see lucrative embezzlement or blackmail opportunities in financial and medical records.[29] In fact, hackers pose a significant national

---

1998) <www.monseyny.com/facts>. The most recent estimate of Internet size is 150 million users worldwide, with 87 million of those from the United States and Canada. *See* NUA Internet Surveys, *How Many Online?* (visited Nov. 20, 1998) <http://www.nua.ie/surveys/how_many_online/index.html>.

[24] *See* Plaintiff's Motion for Summary Judgment at 16, Junger v. Daley, 8 F. Supp.2d 708 (N.D. Ohio 1997) (No. 96 CV 1723) (visited Jan. 20, 1998) <http://www.jya.com/pdj4.htm> (describing the dire consequences of encryption regulation as viewed by the Association for Computing Machinery).

[25] *See* Lennon, *supra* note 18, at 470 (underscoring that the breadth of "digital information" is limited only by the imagination).

[26] *See* AdvoNet, *PGP is Pretty Good Privacy* (visited Jan. 20, 1998) <http://calebproject.org/pgp.htm> (warning encryption users in China and Iraq that their governments may be suspicious of the technology, as opposed to Singapore and Taiwan where encrypted messages are commonplace).

[27] *See* Lennon, *supra* note 18, at 495 n.198. Michael J. Steen was convicted of trafficking in child pornography via computer. *See id.* The police were particularly upset that co-conspirators were never apprehended, in part because Steen used a system of communicating only in encrypted messages. *See id.*

[28] "Hackers are people known for breaking into computer systems . . . ." Evans, *supra* note 5, at 470. They often cause mischief and even damage to information on those systems. *See id.* Such access to computer systems "generally occurs for one of three reasons: (1) an illegal attack for profit or some other benefit; (2) a malicious attack for revenge; or (3) a partially or totally nondestructive attack perpetrated as a game or challenge." *Id.* What was once considered by many to be a childish prank is now a serious concern to corporations, governments, and law enforcement agencies. *See id.*

[29] *See generally id.* at 470-72 (describing hackers, viruses, and "technical mercenaries").

security risk as the global battlefronts fundamentally change to economic rather than military.[30]

B. The Two Faces of Protection

Presented with financial and privacy risks, businesses have turned to programs which scramble their digital information.[31] The cryptography technology employed generally involves encryption, which scrambles data, and decryption, which unscrambles it.[32] Those companies that have not employed cryptography have either sacrificed security or foregone the Internet's advantages.[33] Beyond business rationales, individuals are growing more concerned with the vulnerability of their digital information.[34] As such, many are turning to encryption to help them keep information on their computer as secure as their real-world valuables.[35] Regardless of the identity of the user, encryption is considered the "cornerstone of personal privacy and on-line security."[36]

---

[30] *See Online Security Issues: Hearing of the Science, Tech. and Space Subcomm. of the Senate Commerce, Science and Transp. Comm.*, 104th Cong. 15 (1996) [hereinafter *Security Hearings*] (testimony of Whitfield Diffie, Sun Microsystems Engineer, warning that "we're in more danger of going broke than of getting overrun"). Diffie's hearing testimony further iterated that "it is very important that we do not squander . . . [our] advantage [in computer and communication products and services] by continuing Cold War regulations." *Id.*

[31] *See* Evans, *supra* note 5, at 481 (quoting Eric Hirschhorn & David Peyton, *Uncle Sam's Secret Decoder Ring*, WASH. POST, June 25, 1992, at A23, which claims that encryption has become a "routine business precaution").

[32] *See infra* notes 55-70 and accompanying text (describing cryptography and its uses).

[33] *See generally* Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (visited Nov. 10, 1997) <http://www.crypto.com/key_study/report.shtml> (discussing the consequences of encryption regulations on Internet and economy growth). This report, completed May 27, 1997, was the output of 11 of the world's foremost cryptography experts. *See id.* They concluded that uncompromised, secure networks are a necessity for the Internet and its users to reach their true potential. *See id.*

[34] In fact, companies have been formed solely to help individuals maintain privacy while using the Internet. TRUSTe is one such company that helps users avoid exposure of their information. *See generally* TRUSTe, *Building a Web you can believe in* (visited Oct. 19, 1998) <http://www.truste.org>.

[35] *See* Evans, *supra* note 5, at 481 n.143 (citing *Weekend Edition* (National Public Radio broadcast, Jan. 3, 1993)).

[36] *Security Hearings*, *supra* note 30, at 30 (testimony of Marc Rotenberg, Director,

The U.S. government recognizes these beneficial encryption applications but has concerns about its deleterious uses.[37] In particular, the National Security Agency (NSA),[38] commissioned by President Truman as an arsenal of communication interception,[39] has fought against availability of cryptographic technology.[40] NSA's concern, along with that of other police agencies, is that efforts to stop terrorists and child pornographers[41] will be thwarted by strong encryption.[42] This concern has led to an NSA campaign influencing regulatory and legislative decisions to limit encryption domestically and abroad.[43] Although domestic encryption is currently legal, NSA's influence has affected export controls.[44] Providers of encryption must adhere to guidelines that require a license for exporting certain encryption formulas and strengths.[45] Encryption and privacy advocates claim such controls are irrational and unconstitutional restraints on speech.[46] Before

---

Electronic Privacy Information Center, noting that the need for information security is clear to most online users). Rotenberg went further to note that online security interest grew during initial government attempts to impose a proprietary encryption solution called the Clipper Chip. *See id.* This chip allowed the government a "backdoor" to all communications which used the Clipper Chip for encryption. *See id.* A grass-roots uprising took hold to defeat that proposal, with 47,000 signatures on electronic petitions opposing the Clipper. *See id.*

[37] *See* Lennon, *supra* note 18, at 472 (noting that the struggle to control encryption is at the heart of tension between the desire to safeguard private information and the desire to preserve law-enforcement capabilities).

[38] *See* Evans, *supra* note 5, at 478 (describing the establishment of the National Security Agency in 1947 and the agency's primary intelligence and communications responsibilities).

[39] *See id.*

[40] *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 156 (describing the influence NSA exerts over commercial cryptography).

[41] *See* Lennon, *supra* note 18, at 495 n.198 (describing dissatisfied police who caught a California on-line child pornographer but never apprehended his co-conspirators because communications were encrypted).

[42] *See infra* notes 394-405 and accompanying text (discussing the key government concern: national security).

[43] *See infra* notes 394-405 and accompanying text (discussing the key government concern: national security).

[44] *See* Evans, *supra* note 5, at 478-79 (describing past and present NSA positions on exporting encryption).

[45] *See infra* notes 98-128 and accompanying text.

[46] *See Security Hearings*, *supra* note 30, *passim*.

analyzing the legal and policy arguments of this debate, it is informative to look at one encryption provider's recent export experience.

C. Pretty Good Publishing

Phil Zimmerman, a Colorado computer programmer, created a product called Pretty Good Privacy (PGP)[47] which enabled users to encrypt and decrypt their email.[48] Because of strong beliefs about an individual's right to privacy, and possibly to create a de facto standard, he created free versions of his programs for anyone to use.[49] After various difficulties with the authorities in exporting his early versions, Zimmerman decided to publish his most recent version, PGP 5.0, in twelve volumes of print form.[50] Although he claims the volumes were printed to allow peer review of his algorithms, the printing also allowed for access to a loophole in the export restrictions.[51] Because his algorithms were so difficult to break, export regulations did not allow export of his code by disk or the Internet.[52] However, in recognition of free expression principles, the regulations permitted exporting the same code in

---

[47] PGP is now one of the most widely used products for secure communications. *See* Thinh Nguyen, Note, *Cryptography, Export Controls, and the First Amendment in* Bernstein v. United States Department of State, 10 HARV. J.L. & TECH. 667, 679 n.91 (1997).

[48] *See id.*

[49] *See generally* Philip R. Zimmerman, *Foreword to the First Volume* of PRETTY GOOD PRIVACY 5.0 PLATFORM INDEPENDENT SOURCE CODE (visited Oct. 3, 1998) <http://mail.telstar.net/mirror/pgp/foreword.shtml> (describing Zimmerman's recent legal battles and the new features of PGP 5.0). His free-download approach distributed PGP across the globe. *See* Lennon, *supra* note 18, at 495 n.195. For example, it was the eighth most popular piece of software downloaded from a large New York-based software site. *See id.*

[50] *See* Philip R. Zimmerman, *Foreword to the First Volume* of PRETTY GOOD PRIVACY 5.0 PLATFORM INDEPENDENT SOURCE CODE (visited Oct. 3, 1998) <http://mail.telstar.net/mirror/pgp/foreword.shtml> (describing Zimmerman's recent legal battles and the new features of PGP 5.0).

[51] *See infra* notes 125-28 and accompanying text (describing the regulatory exception made for printed material even where the same material in electronic form is restricted).

[52] *See infra* notes 118-22 and accompanying text (noting that publishing encryption programs on a web page requires an export license).

printed form.[53] Thus, within weeks of Zimmerman's releasing PGP 5.0 in the United States, a group in Norway legally received the printed books and scanned in the code to create PGP 5.0i, the international edition.[54] For some this was a triumph for privacy, for others a defeat for national security. Either way, it highlights the disputed distinctions that exist in the current encryption export regulations.

II. Encryption and Export: A Foundation

To understand the issues being raised in judicial and legislative proceedings about encryption, it is imperative to investigate the history and terms of the science of cryptography. Furthermore, to advise an encryption exporter, one must be familiar with the technology distinctions in the regulations and the process required to obtain a license.

A. A Cryptography Primer

1. Cryptography and Its Uses

The term "cryptography" stems from ancient Greek roots signifying "hidden writing;"[55] generally, cryptography means writing in a secret manner.[56] The benefits of cryptography have been recognized for centuries.[57] For example, the Greeks and Romans disguised messages[58] as did our founding fathers, Thomas Jefferson and James Madison.[59] Encryption is the process of

---

[53] *See id.*

[54] *See PGP 5.0 exported!* (visited Oct. 3, 1998) <http://www.pgpi.com/project/pgp50.shtml> (describing the scanning process and the international anticipation of PGP 5.0i as "encryption for the masses").

[55] SHAWN JAMES ROSENHEIM, THE CRYPTOGRAPHIC IMAGINATION 19 (1997).

[56] *See generally id.*

[57] *See id.*

[58] *See* Evans, *supra* note 5, at 472 n.31 (noting that early Greeks and Julius Caesar used encryption techniques to protect confidential messages (citing PER CHRISTOFFERSSON ET AL., CRYPTO USERS' HANDBOOK 88 (1988))).

[59] *See* Rachel E. Schwartz, *US Courts Split on Restricting Encryption Software*, LAW JOURNAL EXTRA!, July/Aug. 1997, at 1 (visited Nov. 15, 1997) <http://www.ipww.com/jul97/p31us.html> (noting that Bill of Rights author James Madison used a cipher devised by Thomas Jefferson for communication while in

transforming a message, called plaintext, into some unreadable form, known as ciphertext.[60] This is done by applying a cryptographic algorithm to the text.[61] Decryption is the process of reversing the transformation in a manner to reveal the original plaintext message.[62]

The National Research Council (NRC) has identified four major uses of cryptography: "ensuring data integrity, authenticating users, facilitating nonrepudiation (the linking of a specific message to a specific sender) and maintaining confidentiality."[63] The attractions of confidentiality and protecting assets are widely known, but additional benefits of encryption stem from its data integrity, authentication, and non-repudiation features for digital signatures.[64] The lack of secure authentication has hindered the effort for computers to replace paper, and some feel that digital signatures are the exact tool necessary to move the most essential paper-based documents to digital electronic media.[65]

The methods, like the benefits, of performing cryptography vary. Although early cryptography depended on the secrecy of the algorithm for its protection,[66] more powerful, recent versions allow the algorithm to be known and, indeed, encourage attack.[67] This is possible because the secret is found in the user's key and not in the algorithm.[68] The key and the plaintext are supplied to a non-

---

France).

[60] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 1 (1994).

[61] *See id.* at 2.

[62] *See id.* at 1.

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

[64] *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 11-12.

[65] *See id.* at 33 (describing digital signature uses for items such as leases, wills, passports, transcripts, checks, and voter registration).

[66] These algorithms are called "restricted" and are considered "woefully inadequate" for today's security needs. *See* SCHNEIER, *supra* note 60, at 2.

[67] *Cf.* CRYPTOGRAPHY FAQ, *supra* note 7, at 37. The Digital Signature Algorithm published by the National Institute of Standards and Technology (NIST) received criticism for its secretive and arbitrary process that allowed little scrutiny of the algorithm involved. *See id.*

[68] *See* SCHNEIER, *supra* note 60, at 2-4 (describing the role keys play in modern encryption systems).

restricted algorithm to produce the ciphertext.[69] The two most widely used systems are secret-key and public-key.[70]

2. Secret-Key Algorithms

Secret-key algorithms exist when "the encryption key can be calculated from the decryption key and vice versa."[71] However, such calculation is unnecessary if the encryption and decryption keys are identical. The process for using a secret-key algorithm involves: (1) agreeing on a secret key with the intended receiver or sending her the key; (2) supplying plaintext and the key to an algorithm to create the ciphertext; (3) sending the ciphertext to the receiver; and (4) having the receiver supply the ciphertext and the key to an algorithm to create the plaintext.[72] The main obstacle with a secret-key approach is reaching a consensus on the secret key without anyone, except the sender and receiver, finding out.[73] When the sender and the receiver are in different locations, they may be forced to rely on couriers, phone systems, or other forms of communication to exchange the key.[74] To minimize the effect of a compromised key, some systems create a new random key for every exchange.[75]

The most widely used cryptosystem in the world is the Data Encryption Standard (DES).[76] The system utilizes a secret-key algorithm created by the IBM Corporation,[77] which was adopted as

---

[69] *See id.* at 3 (diagramming the process of encryption and decryption with key in Figure 1.2).

[70] *See id.* at 3-4.

[71] *Id.* at 3.

[72] *See generally* CRYPTOGRAPHY FAQ, *supra* note 7, at 17 (describing problems with secret key approaches).

[73] *See id.*

[74] *See id.*

[75] *See id.* at 93. A One Time Pad (OTP) algorithm is an example of this. *See* Michael Paul Johnson, *Data Encryption Software and Technical Data Controls in the United States of America* § 4.8 (last modified Jan. 7, 1994) <http://www.eff.org/pub/Privacy/ITAR_export/cryptusa.paper> (providing a short sample implementation of a OTP encryption algorithm).

[76] *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 66. Alternatives to this standard are the RC5, SAFER, and Skipjack algorithms. *See id.* at 76, 78, 80.

[77] *See id.* at 66.

a federal standard on November 23, 1976 and subsequently has been re-certified every five years.[78] The key used for the endorsed standard has a length of fifty-six bits.[79] Since brute-force attacks[80] depend on trying various key combinations, an increased key length yields greater protection from attack.[81] Although a 56-bit key length appeared virtually impossible to break in 1994, it is now believed that a computer designed to crack DES can do so in just three and a half hours.[82]

3. Public-Key Algorithms

Public-key algorithms attempt to solve the secret-key management problem by providing each person a pair of keys: a public key and a private key.[83] A receiver's public key, which is used for encryption, can be published for all to see, whereas the private key, which is used for decryption, must be heavily guarded.[84] Because the private key is not needed by both parties, it never needs to be transmitted between the parties as do secret-keys.[85] The process for such an algorithm involves: (1) obtaining a receiver's public key; (2) supplying plaintext and the public key to an algorithm to create the ciphertext; (3) sending the ciphertext to the receiver; and (4) having the receiver supply the ciphertext and her private key to an algorithm to re-create the plaintext.[86]

---

[78] *See* SCHNEIER, *supra* note 60, at 221-24. It has been suggested that 1993 was the final renewal that standard will receive. *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 66.

[79] *See* SCHNEIER, *supra* note 60, at 236 (noting that original designs called for a 128-bit key but the NSA felt 56-bit keys were sufficiently secure).

[80] *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 61 (describing "brute-force" or exhaustive key search attacks).

[81] *See id.*

[82] *See* Evans, *supra* note 5, at 473 n.45 (describing the $1 million computer required and noting that a $1 billion computer could succeed with a brute-force attack in just 13 seconds (citing Bruce Schneier, *The Cambridge Algorithms Workshop*, DR. DOBB'S J., Apr. 1994, at 22 (1994))); *see also* Johnson, *supra* note 75, at § 4.7 (claiming that "DES was doomed to a limited lifetime from the beginning by limiting its key length to 56 bits.").

[83] *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 17.

[84] *See id.*

[85] *See id.*

[86] *See generally* SCHNEIER, *supra* note 60, at 4 (describing the benefits of

This approach provides security and convenience, and has the added benefit of enabling digital signatures.[87] However, the main disadvantage of this method is the slow speed.[88] To solve the speed problem many solutions use fast secret-key methods to encrypt full messages and use public-key methods to encrypt exchange of the secret key.[89]

The most popular public-key system is the RSA system developed in 1978.[90] Because of the algorithm, the key lengths are not comparable to DES in terms of strength. Rather, the security of RSA depends on the difficulty in factoring extremely large numbers.[91] With direct attacks on a strong 1024-bit RSA implementation taking ten billion years, it is highly probable that attack efforts will instead focus on uncovering the receiver's private key.[92]

4. Key Management Terminology

Although many of the policy issues surrounding key management are discussed in Part V of this Comment, it is important to provide an overview of the terms used in the discussion. As a police modification to secret-key and public-key systems, sometimes "key recovery" is requested.[93] Although it is referred to by various names, generally key recovery means "any system . . . guarantee[ing] law enforcement agencies timely access,

---

introducing public and private keys).

[87] *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 19 (noting that public-key authentication gives each user the responsibility of protecting her private key which is crucial for no-repudiated digital signatures).

[88] *See* SCHNEIER, *supra* note 60, at 285 (noting that the most common public-key algorithm "is about 1000 times slower than DES").

[89] *See id.*

[90] *See id.* at 281-82. (describing the algorithm and its namesake inventors: Ron Rivest, Adi Shamir, and Leonard Adleman). By 1996 RSA was licensed to over 150 companies and claimed an installed base of 20 million users. *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 31.

[91] *See* SCHNEIER, *supra* note 60, at 284 (mentioning that the "most paranoid" use 1024-bit RSA algorithms requiring prime numbers with 308 digits).

[92] *See id.*

[93] Today the term "key recovery" is used generically to represent a variety of recovery schemes such as key escrow, trusted third-parties, exceptional access, and data recovery. *See* Abelson et al., *supra* note 33, at Executive Summary.

without user notice, to the plaintext of encrypted communications traffic."[94] For any given system, this request is not technically prohibitive, but complexity increases as a global infrastructure is attempted.[95] Such key recovery systems rely on key escrow agents to hold the private keys of all of its members.[96] Some systems may also employ key sharing, where escrow agents holds parts of user private keys.[97]

B. An Export Primer

1. Regulatory History

Today's encryption export controls first appeared in 1949 when the United States implemented regulatory controls to "prevent the Soviet Union and the Warsaw Pact countries from obtaining Western technology that could enhance . . . [their] military potential."[98] These controls were implemented by enacting the Export Administration Act (EAA)[99] and the Export Administration Regulations (EAR).[100] The regulations state that the Department of Commerce is to use a Commerce Control List (CCL) to classify items for export.[101] The list is divided into ten categories: "Nuclear Materials, Facilities and Equipment and Miscellaneous; Materials, Chemicals, 'Microorganisms,' and Toxins; Materials Processing; Electronics; Computers; Telecommunications and Information Security; Lasers and Sensors; Navigation and Avionics; Marine; and Propulsion

---

[94] *Id.* at § 1.2.

[95] *See id.* at § 3.2.1 (concluding that "[w]e simply do not know how to build a collective secure key-management infrastructure of this magnitude, let alone operate one.").

[96] *See id.* at Executive Summary.

[97] *See* CRYPTOGRAPHY FAQ, *supra* note 7, at 102.

[98] Evans, *supra* note 5, at 474.

[99] *See* Export Administration Act of 1979, Pub. L. No. 96-72, 93 Stat. 503 (codified as amended at 50 U.S.C. app. 2401-2420 (1988 & Supp. III 1991)).

[100] *See* Export Administration Regulations, 15 C.F.R. §§ 730-774 (1998).

[101] *See* Evans, *supra* note 5, at 474-76 (describing the CCL and its international underpinnings from the Coordinating Committee on Multilateral Export Controls (COCOM)); *see also* 15 C.F.R. § 738 (1998).

Systems, Space Vehicles and Related Equipment."[102] The CCL explains what controls are imposed, which countries are limited, and what license an exporter needs to sell her products overseas.[103]

Although encryption items are currently controlled by EAR through the Department of Commerce, it is important to note that, at one time, they were controlled under the Arms Export Control Act (AECA)[104] and the International Traffic in Arms Regulations (ITAR).[105] Under ITAR, the Department of State controlled encryption exports as defense articles on the United States Munitions List (USML) until 1996.[106] The only three cases to challenge encryption export restrictions were all brought before non-military encryption items were moved back under EAR control.[107] Although the Executive Order transferring encryption items from the USML to EAR control was part of President Clinton's promised "sweeping changes in . . . export controls,"[108] software industry representatives and civil libertarian groups viewed the move as "a pointless shell game."[109] As the focus of this Comment is on the EAR regulations as they exist today and in the future, any ITAR similarities have little substantive effect on

---

[102] 15 C.F.R. § 738.2(a) (1998). These categories are then further divided into five groups: Equipment, Assemblies and Components; Test, Inspection and Production Equipment; Materials; Software; and Technology. *See id.* at § 738.2.(b).

[103] *But see* Evans, *supra* note 5, at 476 (noting that "software is scattered throughout the CCL, making it much more difficult to identify which software products are subject to export controls").

[104] *See* 22 U.S.C. § 2751 (1994).

[105] *See* 22 U.S.C. § 2778(a)(1) (1994); 22 C.F.R. §§ 120-130 (1998).

[106] *See* 22 U.S.C. § 2778 (describing the USML); *see also* Exec. Order No. 13,026, 3 C.F.R. 228 (1998), *reprinted as amended in* 50 U.S.C.S. app. § 2403 (Law. Co-op. 1998) (noting that encryption items transferred from the USML prior to Nov. 15, 1996 are not controlled as encryption items).

[107] *See infra* notes 129-272 and accompanying text (describing encryption cases attacking ITAR which turned to EAR after the regulatory shift).

[108] Remarks Announcing a National Export Strategy and an Exchange With Reporters, 29 WKLY. COMP. PRES. DOC. 1918, 1919 (Sept. 29, 1993).

[109] Bill Pietrucha, *Professor Wants Constitutional Review of Cryptography* (visited Oct. 19, 1998) <http://www.info-sec.com/crypto/infosecz.html-ssi> (quoting John Gilmore, co-founder of the Electronic Frontier Foundation). This industry pessimism resulted from the timing of the Executive Order. The Order came only days before a California District Court ruled the ITAR provisions were unconstitutional prior restraints. *See id.*; *see infra* notes 172-73 and accompanying text.

the legal principles discussed.

2. Encryption Item Classifications

The new EAR regulations added a category called "Encryption Items" (EI) as a reason for control.[110] This category includes "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR."[111] The EI regulations also included three sub-categories of items falling under telecommunications and information security that are controlled for EI reasons: encryption commodities, encryption software, and encryption technology.[112] Notably, these classifications do not include software that employs encryption only for authentication, encryption of passwords or personal identification numbers, or certain banking or money machine functions.[113] Further, the classifications also consider whether items are "recovery encryption software and equipment,"[114] which are legally entitled by government officials to obtain the plaintext of encrypted data and communications.[115] With the shift of items to the CCL also came some encryption-specific exceptions to the usual rules on software. Three noteworthy exceptions involve the regulation of free software, the definition of export, and the foreign availability impacts.

Before Executive Order 13,026, the EAR traditionally did not impose any controls on software under its jurisdiction if the software was freely available to any party.[116] However, a key provision carried over from ITAR imposes full export control jurisdiction over all encryption software, even software that is otherwise available for free without any restriction.[117] Given the

---

[110] *See* 15 C.F.R. § 738.2(d)(2)(i)(A) (1998).

[111] 15 C.F.R. § 772 (1998).

[112] *See* 15 C.F.R. § 742.15 (1998) (describing new categories ECCN 5A002, ECCN 5D002, and ECCN 5E002, respectively).

[113] *See* Fred M. Greguras & John Black, *Internet Export Compliance Issues for Software* § II(A) (visited Nov. 2, 1997) <http://www.jya.com/inetxport.htm>.

[114] 15 C.F.R. § 742.15(b)(2).

[115] *See id.*

[116] *See* Greguras & Black, *supra* note 113, § II.

[117] *See id.*

proliferation of free software on the Internet, this provides distinctly broader control over encryption products than other software technologies.

The second encryption-specific exception in the new EAR regulations addresses the definition of "export." For non-encryption software, export means "a shipment or transmission of items . . . out of the U.S.; or a 'release' of technology or source code to a foreign national in the U.S."[118] This differs from encryption software, where "export" also includes: "downloading, or causing the downloading of software to locations . . . outside the U.S.; or making such software available for transfer outside the U.S., . . . including transfers from electronic bulletin boards, Internet file transfer protocol and *WWW sites*."[119] According to this definition, publishing software on a web page is considered an export only when that software fits the EAR definition of encryption software.[120] An exception is provided for such publishing where "the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside of the United States."[121] Compliance procedures must either be pre-approved by the Commerce Department's Bureau of Export Administration (BXA) or must control access by human or automated means that:

> checks the address of every system requesting or receiving a transfer and verifies that such systems are located within the U.S.; provides every requesting or receiving party with notice that the transfer includes or would include cryptographic software subject to export controls under the EAA and that anyone receiving the transfer may not export the software without a license; and [requires] every party requesting or receiving a transfer of such software . . . [to] acknowledge

---

[118] *Id.* at § III(C)(1).

[119] *Id.* at § II(B) (emphasis added).

[120] *But see* Greguras & Black, *supra* note 113, § III(C)(1) (mentioning that the Bureau of Export Administration interprets "export" to include Internet access even for non-encryption software when the provider receives information or "Red Flags" that foreign parties are downloading). Although this interpretation appears to level encryption and non-encryption software regulations, it is unlikely that "Red Flags" would ever appear in the automated download environment of the Internet.

[121] 15 C.F.R. § 734.2(b)(9)(B)(ii) (1998).

> affirmatively that he or she understands that cryptographic software is subject to export controls under the EAA and that anyone receiving the transfer may not export the software without a license.[122]

In addition to the free software and export distinctions, availability of equivalent foreign technology affects encryption software differently than other software. Before the addition of encryption software, all software on the CCL was excepted from export control if that software was already available in foreign countries.[123] However, as encryption software moved to the CCL, this foreign availability exception became limited only to non-encryption software. As stated by President Clinton:

> [E]xport of encryption products . . . [may] harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States . . . . [P]rovisions of the EAA relating to foreign availability, and the regulations in the EAR relating to such EAA provisions, shall not be applicable with respect to export controls on such encryption products.[124]

One further encryption-specific provision added to the EAR involves electronic publishing as opposed to printed material. Section 734.3(b)(2) of the EAR states that "a printed book or other printed material setting forth encryption source code is not itself subject to the EAR."[125] However, "encryption source code in electronic form or media . . . remains subject to the EAR."[126] Thus, source code in a book is not controlled by the EAR, whereas the same source code on a computer disk may be forbidden or require

---

[122] Greguras & Black, *supra* note 113, § II(C).

[123] *See* 15 C.F.R. § 768 (1998).

[124] Exec. Order No. 13,026, 3 C.F.R. 228 (1998), *reprinted as amended in* 50 U.S.C.S. app. § 2403 (Law. Co-op. 1998). In addition to making this distinction, the administration also took the position that determining foreign availability was a subject of national security and thus, "facts and questions concerning the foreign availability of such encryption products cannot be made subject to public disclosure or judicial review." *Id.*

[125] 15 C.F.R. § 734.3(b)(3) (1998) (quoting Note to Paragraphs (B)(2) and (B)(3) of this section).

[126] *Id.*

a license under the EAR.[127] The administration continues to review this distinction and has "reserv[ed] the option to impose export controls on [scannable encryption source code] for national security and foreign policy reasons."[128]

III. Challenge in the Courts

The increased regulatory focus on encryption products spawned an inevitable increase in export restriction challenges. In particular, three cases have been decided in the last two years that will shape the encryption export debate for years to come: *Bernstein v. U.S. Department of State*,[129] *Karn v. U.S. Department of State*[130] and *Junger v. Daley*.[131] Although the key constitutional issues will be discussed in Part IV,[132] Part III describes the background and primary holdings for each of these important cases.

A. The Bernstein *Quartet*

Daniel Bernstein, a Ph.D. candidate in mathematics at the University of California at Berkeley, worked in an area of applied mathematics, cryptography, that seeks to develop confidentiality in electronic communications.[133] As part of his graduate studies, "Bernstein developed an encryption algorithm he call[ed] 'Snuffle.'"[134] He articulated that algorithm in an academic paper written in English and in source code written in "C," a high-level programming language.[135] The source code resided in two files,

---

[127] This regulatory anomaly was at the heart of an export restriction challenge in Washington. *See infra* notes 204-09 and accompanying text.

[128] Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,573 (1996) (to be codified at 15 C.F.R. §§ 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772, 774).

[129] *Bernstein I*, 922 F. Supp. 1426 (N.D. Cal. 1996). There are actually four decisions originating from Bernstein's dispute. *See infra* notes 133-203.

[130] 925 F. Supp. 1 (D.D.C. 1996).

[131] 8 F. Supp.2d 708 (N.D. Ohio 1998).

[132] *See infra* notes 274-388 and accompanying text.

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

[134] *Id.* at 1429.

[135] *Id.*

"Snuffle.c" and "Unsnuffle.c," which described the procedures for encryption and decryption, respectively.[136] Once the source code was converted into "object code" through the use of compilers,[137] a computer could read the code and encrypt and decrypt data for a user.[138] On June 30, 1992, Bernstein submitted a Commodity Jurisdiction Request (CJR)[139] to the State Department to determine whether the academic paper and the two source files were controlled by ITAR.[140] After being notified that all items were subject to licensing under ITAR, and following some contentious correspondence on the point, Bernstein submitted a second CJR asking for a separate determination for each of five items: (1) the academic paper; (2) Snuffle.c; (3) Unsnuffle.c; (4) an English description of how to use Snuffle; and (5) English instructions for programming a computer to use Snuffle.c.[141] Upon hearing from the ODTC that all items were defense articles under ITAR, Bernstein began the legal war that has generated four successive battles in the Federal courts.[142]

1. Bernstein I

In addition to appealing the CJR determination, Bernstein brought an action in the Northern District of California seeking declaratory and injunctive relief from enforcement of the AECA and ITAR.[143] Bernstein claimed that those regulations were unconstitutional on their face and as applied to him.[144] In April 1996 Judge Marilyn Hall Patel ruled on the Department of State's

---

[136] *See id.*

[137] *See id.* at 1429 n.3 (describing the differences between source code and object code as well as the translation process performed by compilers).

[138] *See id.* at 1329 nn. 3-4.

[139] A CJR is the formal name for a commodity application submitted to the export governing body. *See* 22 C.F.R. § 120.4 (1998).

[140] *See Bernstein I*, 922 F. Supp. at 1430.

[141] *See id.*

[142] *See infra* notes 143-203 and accompanying text.

[143] *See Bernstein I*, 922 F. Supp. at 1428.

[144] *See id.* at 1430-31. The plaintiff claiming that the ITAR imposed an unconstitutional prior restraint on cryptographic speech, that a number of terms make the ITAR vague and overbroad in violation of the First Amendment, and that the ITAR infringes the rights of association and equal protection. *See id.*

motion to dismiss in *Bernstein I*.[145] In its motion, the defendant relied on AECA language that states: "The designation by the President (or by an official to whom the President's functions . . . have been duly delegated), in regulations issued under this section, of items as defense articles . . . for purposes of this section *shall not be subject to judicial review*."[146] In the alternative, the defendant also claimed that the facts did not present a colorable constitutional claim.[147]

Regarding the clear AECA language, Judge Patel noted that "a review of a particular CJR decision is a distinctly different question from a constitutional challenge to a statute."[148] In finding that Bernstein was challenging the statute rather than the CJR decision, Judge Patel relied on an EAA decision, *United States v. Bozarov*[149] from the Ninth Circuit, which stated that "colorable constitutional claims may be reviewed by the courts even when a statute otherwise precludes judicial review."[150] Her position gained further support from *Webster v. Doe*,[151] in which the Supreme Court stated:

> [W]here Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear . . . . We require this heightened showing in part to avoid the "serious constitutional question" that would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim.[152]

With this foundation, Judge Patel turned to analyze whether a colorable constitutional claim existed. In particular, Judge Patel inquired whether Bernstein's source code was protectable speech

---

[145] *See id.* at 1426.

[146] *Id.* at 1431 (emphasis added) (quoting 22 U.S.C. § 2778(h)).

[147] *See id.* at 1432-33. Colorability, though often employed by the courts, is rarely defined. The Ninth Circuit applied a standard that a "constitutional claim is not colorable if it is clearly immaterial and made only for the purpose of jurisdiction, or 'is wholly insubstantial or frivolous.'" *Id.* (citing Hoye v. Sullivan, 985 F.2d 990, 991-92 (9th Cir. 1992)).

[148] *Id.* at 1431.

[149] 974 F.2d 1037 (9th Cir. 1992).

[150] *Id.* at 1044 (citing Webster v. Doe, 486 U.S. 592, 602-05 (1988)).

[151] 486 U.S. 592 (1988).

[152] *Id.* at 603 (citations omitted).

under the First Amendment.[153] The defendant urged the court to find the Snuffle source code unprotected conduct that was not "'sufficiently imbued with the elements of communication' to fall within the protections of the First Amendment."[154] Even if such conduct was expressive, the defendant argued that "the relatively mild *O'Brien* test should be employed."[155] The *O'Brien* test allows regulation of conduct that incidentally restricts speech where: "(1) it is within the power of government; (2) it furthers an important or substantial government interest; (3) the government interest is unrelated to the suppression of expression; and (4) the incidental restriction on speech is no greater than is essential to further that interest."[156]

In what may be the most far-reaching and significant holding of all the encryption export cases, Judge Patel rejected the government's arguments and found software to be protectable expression under the First Amendment.[157] More specifically, the court relied on a Ninth Circuit decision, *Yniguez v. Arizonians for Official English*,[158] in distinguishing expressive conduct from speech in the context of non-English languages.[159] That court stated:

> Of course, speech in any language consists of the 'expressive conduct' of vibrating one's vocal chords, moving one's mouth and thereby making sounds, or of putting pen to paper, or *hand to keyboard.* Yet the fact that such 'conduct' is shaped by language—that is, a sophisticated and complex system of understood meanings—is what makes it speech. Language is by definition speech, and the *regulation of any language is the*

---

[153] *See Bernstein I*, 922 F. Supp. at 1432-36. Although initial CJR determinations also disallowed export of Bernstein's academic papers, the State Department reversed their position after Bernstein filed suit. *See id.* at 1434. Judge Patel found it "disquieting" that such papers were reclassified only after plaintiff initiated action. *Id.*

[154] *Id.* at 1434 (quoting Texas v. Johnson, 491 U.S. 397 (1989)).

[155] *Id.* at 1436 (citing United States v. O'Brien, 391 U.S. 367 (1968)).

[156] *Id.* at 1436-37.

[157] *See id.* at 1436.

[158] 69 F.3d 920 (9th Cir. 1995) (vacated on other grounds).

[159] *See Bernstein I*, 922 F. Supp. at 1435.

regulation of speech.[160]

By finding that the Snuffle source code was speech, Judge Patel ruled that the plaintiff alleged "facts sufficient to state a nonfrivolous First Amendment claim and hence that claim is colorable."[161] Closely related to this finding, Judge Patel also ruled that the AECA and ITAR licensing scheme could act as a prior restraint on that mode of speech.[162]

2. Bernstein II

By December 2, 1996, Bernstein had become a Research Assistant Professor at the University of Illinois at Chicago and planned to use his Snuffle code for teaching purposes.[163] Two of his main concerns involved teaching the code to foreigners and publishing it in journals or online discussion groups without a license.[164] As there were no disputes of material fact, Judge Patel's decision addressed cross-motions for summary judgment regarding Bernstein's prior restraint, overbreadth, and vagueness claims.[165] Contrary to *Bernstein I*, which six months earlier cleared up only the justiciability questions, *Bernstein II* reached the merits of the constitutionality claims and appeared to provide the final word on encryption export regulations.[166]

Since the court in *Bernstein I* determined that source code is speech and "both parties agreed that a licensing scheme controls the 'export' of such speech," the *Bernstein II* court turned first to a prior restraint analysis.[167] Judge Patel began by recognizing that

---

[160] *Yniquez*, 69 F.3d at 934-35 (emphasis added) (vacated on other grounds).

[161] *Bernstein I*, 922 F. Supp. at 1437.

[162] *See id.* at 1438. The court also found Bernstein's overbreadth and vagueness claims to be nonfrivolous with little discussion. *See id.* at 1438-39.

[163] *See* Bernstein v. U.S. Dep't. of State (Bernstein II), 945 F. Supp. 1279, 1296 (N.D. Cal. 1996).

[164] *See id.*

[165] *See id.* at 1282.

[166] Although the decision in *Bernstein II* was not appealed, Executive Order 13,026 transferred encryption export responsibility to the Department of Commerce and the EAR so any further disputes had to be relitigated in light of the new regulations. *See* Exec. Order No. 13,026, 3 C.F.R. 228 (1998), *reprinted as amended in* 50 U.S.C.S. app. § 2403 (Law. Co-op. 1998).

[167] *Bernstein II*, 945 F. Supp. 15 2386.

licensing schemes are a form of prior restraint[168] and then applied the *Freedman*[169] test to determine whether there existed procedural safeguards for the licensing scheme to pass constitutional muster.[170] This test used by the Supreme Court requires that:

> (1) any prior restraint to judicial review can be imposed only for a specified brief period during which the status quo must be maintained; (2) expeditious judicial review of that decision must be available; and (3) the censor must bear the burden of going to court to suppress the speech and must bear the burden of proof once in court.[171]

When applying the test to the ITAR scheme, Judge Patel found ITAR to be "a paradigm of standardless discretion, [that] fails on every count."[172] She held that:

> [b]ecause it fails to provide for a time limit on the licensing decision, for prompt judicial review and for a duty on the part of the ODTC to go to court and defend a denial of a license, the ITAR licensing system as applied to [encryption products] acts as an unconstitutional prior restraint in violation of the First Amendment.[173]

In contrast, the court was not as sympathetic to Bernstein's arguments regarding vagueness and overbreadth. Judge Patel noted that vague laws are objectionable for multiple reasons: they fail to provide fair warning to those wishing to act lawfully; they allow for arbitrary and discriminatory application; and they may inhibit First Amendment rights because "uncertainty can cause

---

[168] *See id.* at 1286. While prior restraints have often come in the form of judicial injunctions on publication they are also recognized in licensing schemes. *See* FW/PBS, Inc. v. Dallas, 493 U.S. 215 (1990).

[169] Freedman v. Maryland, 380 U.S. 51, 58-60 (1965).

[170] *See Bernstein II*, 945 F. Supp. at 1286-92.

[171] *FW/PBS*, 493 U.S. at 227 (citing *Freedman*, 380 U.S. at 58-60).

[172] *Bernstein II*, 945 F. Supp. at 1289.

[173] *Id.* at 1290. The holding was somewhat different for Bernstein's technical data claims, regarding teaching to foreigners. Although questioning the currency of the precedent, Judge Patel effectively yielded to Ninth Circuit authority provided by United States v. Edler, 579 F.2d 516 (9th Cir. 1978). *See id.* at 1290-92. That court adopted a narrowing construction to save a statute from prior restraint infirmities. *See Edler*, 579 F.2d at 521.

speakers to say less."[174] However, for a facial vagueness claim to survive, "the deterrent effect of the statute on protected expression must be 'real and substantial' and *not easily narrowed by a court.*"[175] After recognizing that "defense articles," "defense services," and "technical data" have overlapping meanings that can be grounds for vagueness, Judge Patel chose to reword the statute rather than void it.[176] Similarly, plaintiff's uncertainty over the definitions of "technical data" and "exports" did not persuade the court, as it refused to void application with those terms.[177] One section which did garner Judge Patel's support as impermissibly vague was § 120.11(a)(8), which exempted information available to the public "through fundamental research in science and engineering."[178] Citing the likely confusion between cryptographic algorithms published in scientific journals and those requiring governmental approval, the court voided the academic exemption sections for vagueness.[179] The court's consideration of overbreadth was closely tied to its vagueness findings, and accordingly, it held that "neither the definition of export nor the ITAR scheme as a whole is unconstitutionally overbroad."[180]

Finally, Bernstein's request for a preliminary injunction for his teaching activities was denied without prejudice. Judge Patel reasoned that given the government's assertion that teaching a cryptography class did not violate the regulations and that the court found provisions of ITAR were an invalid prior restraint, there was no immediate threat of injury and no need to rule on the preliminary injunction.[181] Judge Patel closed by stating that Bernstein may renew the motion if later threatened with prosecution.[182]

---

[174] *Bernstein II*, 945 F. Supp. at 1292.

[175] *Id.* (emphasis added) (citing Young v. American Mini Theatres, Inc., 427 U.S. 50, 60 (1976)).

[176] *See id.* at 1293.

[177] *See id.*

[178] 22 C.F.R. § 120.11(a)(8).

[179] *See Bernstein II*, 945 F. Supp. at 1294.

[180] *Id.* at 1295.

[181] *See id.* at 1296.

[182] *See id.*

3. Bernstein III

Near the time of Judge Patel's decision holding that the ITAR encryption regulations were unconstitutional prior restraints on speech, President Clinton issued Executive Order 13,026.[183] The order transferred jurisdiction over the export of nonmilitary encryption products to the Department of Commerce pursuant to the EAA.[184] After this Order was implemented, the plaintiff amended his complaint to include the new regulations and new defendants.[185] The case with these new regulations and defendants has become known as *Bernstein III.*

Although trumpeted by the administration as "a plan to make it easier for Americans to use stronger encryption products to protect their privacy,"[186] the transfer provided little change in regulating encryption export. In fact, Judge Patel ultimately reached the same conclusions about EAR as she previously had about ITAR, holding that "the encryption regulations are an unconstitutional prior restraint in violation of the First Amendment."[187]

The defendants did not argue that the regulations were notably different, but instead presented arguments against some of the reasoning in *Bernstein II.* The defendants protested that the plaintiff's facial challenge was not applicable here because there was "not a 'close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of identified censorship risks.'"[188] This test, outlined in *City of Lakewood v. Plain Dealer Publishing,*[189] distinguished between laws directed at expression and those of

---

[183] *See* Bernstein v. U.S. Dep't of State (Bernstein III), 974 F. Supp. 1288, 1291 (N.D. Cal. 1997); Exec. Order No. 13,026, 3 C.F.R. 228 (1998), *reprinted as amended in* 50 U.S.C.S. app. § 2403 (Law. Co-op. 1998).

[184] *See id.*

[185] *See id.*

[186] Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,573 (1996) (to be codified at 15 C.F.R. §§ 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772, 774).

[187] *Bernstein III,* 974 F. Supp. at 1308.

[188] *Id.* at 1304 (quoting the facial challenge test as stated in City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 759 (1988)).

[189] 486 U:S. 750 (1988).

general applicability not aimed at expressive conduct.[190] Judge Patel disagreed with the defendants and found "the most common expressive activities of scholars—teaching a class, publishing their ideas, speaking at conferences, or writing to colleagues over the Internet—are subject to a prior restraint by the export controls when they involve cryptographic code or computer programs."[191]

In the alternative, the defendants noted BXA regulation exceptions for printed materials that could address censorship concerns.[192] Judge Patel afforded no weight to such a concession and even found that it could possibly exacerbate the potential for self-censorship.[193] Further, Judge Patel held the print distinction was irrational and was confounded by the defense explanation that scanning print into software required a good deal of skill.[194] Finally, she held that the print exception undermined the stated purpose of the regulations and that, in light of *Reno v. American Civil Liberties Union*,[195] "not only is the distinction between print and electronic media increasingly untenable, but the Internet is subject to the same exacting level of First Amendment scrutiny as print media."[196]

With holdings similar to *Bernstein II*, Judge Patel afforded the plaintiff injunctive relief but refused to wholly invalidate the regulations.[197] Due to the finding of facial invalidity the court could have ordered nationwide relief, but the novel and complex issues involved warranted Judge Patel's granting of narrow relief pending appeal.[198] The defendants were "enjoined from enforcing

---

[190] *See id.* at 759-62.

[191] *Bernstein III*, 974 F. Supp. at 1305.

[192] *See* 15 C.F.R. § 734.3(b)(2) (1998). For example, these exceptions include printed books, maps, newspapers, and films. *See id.*

[193] *See Bernstein III*, 974 F. Supp. at 1306 (citing 61 Fed. Reg. 68,578 (1996) (to be codified at 15 C.F.R. § 734.3)).

[194] *See id.* (noting that the effect of the dichotomy would be to make it more difficult only for the more inept).

[195] 521 U.S. 844 (1997) (finding that the Internet is the most participative medium available in the world and holding that expression over the Internet deserves a protection of free expression at least equivalent to print media).

[196] *Bernstein III*, 974 F. Supp. at 1306-07.

[197] *See id.* at 1309-10.

[198] *See id.* at 1310.

the regulations against the plaintiff or against anyone who seeks to use, discuss or publish *plaintiff's* encryption program."[199]

4. Bernstein IV

The government appealed the *Bernstein III* order to the Ninth Circuit Court of Appeals whereupon Judge Patel issued a limited order enforcing *Bernstein.*[200] For the first and only time to date, the constitutionality of encryption export regulations was considered by a circuit court. In addition to the Opening and Opposition briefs submitted by the parties, Amicus Briefs supporting Bernstein were submitted by the Electronic Privacy Information Center, the Thomas Jefferson Center for the Protection of Free Expression, the National Computer Security Association, a group of constitutional law professors, and the American Association for the Advancement of Science.[201] Oral arguments were held December 8, 1997 before Judges Myron Bright, Betty Fletcher, and Thomas Nelson.[202] A year later, the three judge panel has yet to issue a decision.[203]

B. The Karn *Experience*

Engineer Philip R. Karn undertook a journey through encryption export regulations and the federal courts, which paralleled the *Bernstein* cases.[204] In early 1994, Karn filed (with the U.S. State Department) a pair of CJRs: one for the printed

---

[199] *Id.* (describing the fact-specific remedy and noting also that the *Bernstein II* order was superseded by this one).

[200] *See* Electronic Frontier Foundation, *Court Allows Unlicensed Crypto Export* (visited Sept. 20, 1998) <http://www.eff.org/pub/Legal/Cases/Bernstein_v_DoS/19970829.pressrel> (press release announcing Judge Patel's limiting order pending review by the Ninth Circuit Court of Appeals).

[201] *See* McGlashan and Sarrail, P.C., *Bernstein Pleadings* (visited Sept. 5, 1998) <http://www.arceneaux.com/mcglash/pleadings.html>.

[202] An unofficial transcript of those oral arguments has been made available by the Electronic Frontier Foundation (EFF). *See* EFF, *Unofficial Transcript* (visited Sept. 5, 1998) <http://www.eff.org/pub/Legal/Cases/Bernstein_v_DoS/Legal/971208_unofficial.transcript>.

[203] *See id.*

[204] Karn v. U.S. Dep't of State, 925 F. Supp. 1 (D.D.C. 1996).

book *Applied Cryptography*[205] which contains cryptographic algorithms, and one for a disk containing a verbatim copy of those same cryptographic algorithms.[206] When export of the book was allowed and export of the disk was denied, Karn filed suit in a case that appeared to highlight the irrational distinctions of ITAR encryption regulations.[207] However, inconsistencies in the regulations made little difference when the legal battle became the justiciability of the issue.[208] Judge Charles R. Richey of the U.S. District Court for the District of Columbia, found the issue to be a "'political question' for the two elected branches under Articles I and II of the Constitution."[209]

Judge Richey's opinion presented a methodical jurisdiction analysis for the regulations and their review. To begin, he established that the AECA authorized the President to control the export of "defense articles" and that authority was properly delegated to the Secretary of State who promulgated the ITAR.[210] That regulation specifically included cryptographic systems and components as defense articles on the munitions list.[211] Karn argued that the diskette algorithms, like the book algorithms, were in the public domain and the commodity jurisdiction procedure improperly considered them a defense article.[212] The question then became whether the case was about reviewing the classification or interpreting the restriction for items classified as defense articles.

Judge Richey viewed this as an attempt to challenge the classification of encryption software as a defense article and quoted ITAR language stating that "designation . . . of items as

---

[205] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (1994).

[206] *See Karn*, 925 F. Supp. at 3-4.

[207] *Id.* at 1. Karn brought the suit to challenge what he considered to be "silly rules" governing export of cryptographic software, including software in the public domain. Philip R. Karn, *The Applied Cryptography Case* (visited Oct. 31, 1997) <http://people.qualcomm.com/karn/export/index.html>.

[208] *See* Karn, 925 F. Supp. at 4-8.

[209] *Id.* at 3 (granting the government's motion to dismiss).

[210] *See id.* at 4-5 (citing 22 U.S.C. § 2778(a)(1) and 22 C.F.R. § 120.1(a)).

[211] *See id.* at 5 (citing 2 C.F.R. § 120.4, category XIII).

[212] *See id.* (citing 22 C.F.R. §§ 125.1, 120.11).

defense articles . . . shall not be subject to judicial review."[213] Karn argued that "there is a presumption in favor of judicial review of agency action absent 'clear and convincing evidence' of legislative intent to preclude it."[214] Judge Richey, however, noted Supreme Court warnings that "this standard is not a rigid evidentiary test but a useful reminder to the courts"[215] and may be overcome by express language or other related factors.[216] Given the express prohibition in the statute, objectives of the AECA,[217] and the potential for introducing inconsistency and confusion, Judge Richey held that judicial review of the issue was barred.[218]

Turning to Karn's alternative argument, Judge Richey considered whether the regulations were an unconstitutional prior restraint on expression.[219] His analysis differed greatly from the *Bernstein* rulings as he concluded that ITAR encryption regulations were constitutional.[220] Here the government won its argument that the regulations were content-neutral[221] and thus must only meet the *O'Brien*[222] test: "whether the regulation is (1) within the constitutional power of the government, (2) 'furthers an important or substantial government interest,' and (3) is narrowly tailored to the government interest."[223] This test generally applies to conduct, therefore, Judge Richey rejected Karn's claim that his

---

213 *Id.* (citing 22 U.S.C. § 2778(h)).

214 *Id.* at 6 (citing Bowen v. Michigan Acad. of Family Phys., 476 U.S. 667, 671 (1986)).

215 *Id.* (quoting Block v. Community Nutrition Inst., 467 U.S. 340, 351 (1984)).

216 *See id.* (citing *Block*, 467 U.S. at 345). Additional factors include the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action involved. *See id.*

217 *See id.* (quoting in part 22 U.S.C. § 2778(a)(1)) (noting the AECA aim to further "world peace and the security and foreign policy" of the United States).

218 *See id.* at 6-8.

219 *See id.* at 9-13.

220 *See id.* at 12-13.

221 This conclusion was opposite that of the *Bernstein* court, where the regulations were considered content-based. *See* Bernstein v. U.S. Dep't of State (Bernstein I), 922 F. Supp. 1426, 1436-37 (N.D. Cal. 1996).

222 United States v. O'Brien, 391 U.S. 367 (1968). *See also infra* notes 316-18 (describing the O'Brien test).

223 *Karn*, 925 F. Supp. at 10 (quoting in part *O'Brien*, 391 U.S. at 377).

diskette was "pure speech."[224] Applying the *O'Brien* test, the court held that all three criteria were met; thus the regulations did not violate the Constitution.[225] On the grounds that the court could not decide political questions, Judge Richey also declined to consider Karn's argument that the goal of national security was not furthered because of foreign availability.[226] Karn's remaining arguments, which Judge Richey termed "last-ditch,"[227] were rejected and the defendants were awarded a dismissal on the regulatory authority issue and summary judgment on the plaintiff's constitutional claims.[228] Philip Karn subsequently appealed the government's victory, but Executive Order 13,026 prompted the parties to restart the licensing process under the new EAR scheme.[229] Judge Louis Oberdorfer replaced Judge Richey to hear further disputes in the matter.[230] In April 1998, Karn's CJR was formally rejected and he submitted an amended complaint to Judge Oberdorfer.[231] The government has also filed a motion to dismiss.[232]

C. *The Recent* Junger *Bid*

Professor Peter D. Junger from Case Western Reserve Law School filed the most recent challenge to the encryption export regulations.[233] To aid in teaching his course "Computers and the Law," Junger used encryption programs[234] and a course book

---

[224] *Id.*

[225] *See id.* at 11.

[226] *See id.* at 10-12.

[227] *Id.* at 12.

[228] *See id.* at 12-14 (finding Karn's vagueness and Fifth Amendment arguments unpersuasive).

[229] *See* Philip A. Karn, *Detailed History of the Applied Cryptography Case* (visited Oct. 18, 1998) <http://people.qualcomm.com/karn/export/history.html>.

[230] Judge Richey passed away in March, 1997. *See id.*

[231] *See id.*

[232] *See id.*

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

[234] Professor Junger created a short one-time pad algorithm and referenced other sample encryption programs for teaching purposes. Telephone Interview with Peter Junger, Plaintiff (Nov. 2, 1997).

which contained encryption source code.[235] Further, he wrote a law review article on encryption and maintained a web page with links to domestic and foreign encryption sites.[236] Use of these items was potentially an export, as defined by BXA, and thus, Junger submitted CJRs for all of them.[237] The programs, with the exception of a one-time pad algorithm Junger created,[238] were "classified as 'EI' software, meaning that they could not be exported without a license."[239] This classification meant that any electronic publication of the programs in Junger's course book or law review article would violate the EAR as export without a license.[240] In *Junger v. Daley*,[241] Professor Junger sought injunctive and declaratory relief from the government's enforcement of export controls on encryption software.[242] The case was heard July 2, 1998 in the District Court for the Northern District of Ohio by Judge James S. Gwin.[243]

Professor Junger and the U.S. Secretary of Commerce filed cross-motions for summary judgment in the case based primarily on the interpretation of the First Amendment.[244] The arguments for each side were substantially similar to those presented in the

---

[235] Plaintiff's Motion for Summary Judgment at 4, Junger v. Daley, 8 F. Supp.2d 708 (N.D. Ohio 1997) (No. 96 CV 1723) (visited Nov. 2, 1997) <http://www.jya.com/pdj4.htm>.

[236] *See generally id.* at 19.

[237] *See id.* at 3. Professor Junger also submitted five descriptions of encryption programs. *See id.* These items were refused because none of them identified a specific software program. The BXA Director noted that "licensing controls on encryption software that does not maintain the secrecy of information may vary depending on how the algorithm is implemented in the software." *Id.* at 4 (citation omitted).

[238] *See supra* note 75 and accompanying text (discussing the category of algorithms that includes one-time pads).

[239] Plaintiff's Motion for Summary Judgment at 4, Junger v. Daley, 8 F. Supp.2d 708 (N.D. Ohio 1997) (No. 96 CV 1723) (visited Nov. 2, 1997) <http://www.jya.com/pdj4.htm>.

[240] *See id.* (noting that Junger's encryption programs would have to be removed before his book was published on a website).

[241] 8 F. Supp.2d 708 (N.D. Ohio 1998).

[242] *See id.*

[243] *See id.*

[244] *See id.* at 711.

Bernstein series of cases.[245] Professor Junger's five-count complaint claimed: (1) the export licensing scheme worked a prior restraint on his right to publish scholarly materials; (2) the export regulations were unconstitutionally overbroad and vague; (3) the export regulations engage in unconstitutional content discrimination; (4) the export regulations restrict his academic freedom and freedom of association; and (5) the executive regulation of encryption software under the International Emergency Economic Powers Act[246] violated the separation of powers doctrine.[247] Along with counts 4 and 5, which were decided on non-constitutional grounds,[248] Judge Gwin rejected each of Junger's constitutional attacks on the export regulations.[249] The result was a decision that viewed *Bernstein*-like facts and arguments from a different, and possibly less technically savvy, perspective, and provided a significant split of federal judicial opinion.

After setting forth the applicable legal standards, Judge Gwin addressed the question of whether encryption software is constitutionally protected expression.[250] Because encryption software, when run on a computer, can be functional, the court categorized it as "occasionally expressive conduct" rather than "speech."[251] The court looked for an "overwhelmingly apparent"[252]

---

[245] *See supra* notes 133-203 and accompanying text (describing the competing arguments and resolutions in the *Bernstein* cases).

[246] *See Junger*, 8 F. Supp.2d at 712 (citing 50 U.S.C. § 1701).

[247] *See id.* at 711-12.

[248] *See id.* at 720-23. Because academic freedom and freedom of association were not addressed in the submitted briefs, Judge Gwin considered that argument waived by Junger. *See id.* at 723. The separation of powers question was settled by the court claiming a lack of jurisdiction to review the President's authority. *See id.* (citing Dalton v. Specter, 511 U.S. 462, 474 (1994), which states "that such review is not available when the statute in question commits the decision to the discretion of the President.").

[249] *See id.* at 715-20.

[250] *See id.* at 715-18.

[251] *Id.* at 717 (citing City of Dallas v. Stanglin, 490 U.S. 19 (1989)). Note, however, that this approach presumes treatment of software as conduct rather than speech. By the court's own admission, "[w]hether the alleged 'speech' is actually expressive is immaterial if it is communicated through language." *Id.* at 716. A critical assumption by the court which goes unsupported, is that computer "language" is not a language even though the court admits that computer scientists use it to do their

or "unmistakable message"[253] in the expressive elements of encryption source code and failed to find one.[254] This determination was critical to Judge Gwin's analysis as he proceeded to the issue of prior restraint. Citing *City of Lakewood v. Plain Dealer Publishing Co.*,[255] the court rejected Junger's facial challenge to the export regulations because such an attack "is appropriate only where the challenged statute 'is directed narrowly and specifically at expression or conduct commonly associated with expression.'"[256] The court found that the export regulations were not narrowly directed at expressive conduct and, therefore, were not a prior restraint.[257]

Turning to Junger's overbreadth and vagueness claim, the court noted that such "challenges are 'strong medicine' that should be used 'sparingly and only as a last resort.'"[258] Further, the court adhered to the rule that overbreadth attacks are inapplicable "where the law effects [sic] the plaintiff and third parties in the same manner."[259] Judge Gwin ruled that the potential injury to Junger was the same as that to "other academics."[260] Thus, the

---

research. *See id.* at 717 (conceding that "trained computer programmers can read and write in source code").

[252] *Id.* (citing Texas v. Johnson, 491 U.S. 397, 406 (1989)).

[253] *Id.* (citing Tinker v. Des Moines Indep. Community Sch. Dist., 393 U.S. 503, 506 (1969)).

[254] *See id.* Evidently, submissions by Junger that many people used source code to communicate messages carried little weight with Judge Gwin. *See* Email Interview with Cindy A. Cohn, McGlashan & Sarrail, P.C. (Sept. 8, 1998) (on file with author) [hereinafter Cohn Email]. It appears that Judge Gwin considered the number of people who understand a message to be a proxy for the gravity of its expressive element. However, Judge Gwin presented no authority for the implied assumption that the number of people who communicate in a given language is critical in deciding whether that communication is speech. *See id.*

[255] 486 U.S. 750 (1988).

[256] *Junger*, 8 F. Supp.2d at 718 (quoting City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 760 (1988)).

[257] *See id.* at 719.

[258] *Id.* (citing New York State Club Ass'n, Inc. v. City of New York, 487 U.S. 1, 14 (1988) (quoting Broadrick v. Oklahoma, 413 U.S. 601, 613 (1988))).

[259] *Id.*

[260] *Id.* By considering only "other academics" Judge Gwin ignored declarations submitted by Junger that non-academics had been injured in various ways by the export regulations. *See* Cohn Email, *supra* note 254.

court found such injury could not be the basis of an overbreadth challenge.[261] Junger's claim of vagueness was likewise dismissed as Judge Gwin felt that the regulations were sufficiently detailed.[262]

Finally, Junger's content discrimination claim was rejected in a two-part analysis focusing on level of scrutiny and application of that scrutiny.[263] The court looked first at the appropriate level of scrutiny for the encryption export regulations.[264] Contrary to Junger's assertion that strict scrutiny should apply, the court felt intermediate scrutiny was appropriate because it found the export regulations to be content neutral.[265] The overriding factor in this determination was the government's purpose.[266] Even though encryption software is subject to a stricter standard than other software, Judge Gwin was satisfied that the regulations targeted "encryption software [function] without reference to any views it may express."[267] The court also applied this reasoning to reject Junger's claim that allowing print but not electronic export of encryption software was media discrimination contrary to *Reno v. American Civil Liberties Union*.[268] Much like the *Karn* court, Judge Gwin applied intermediate scrutiny, and specifically the

---

[261] *See Junger*, 8 F. Supp.2d at 719.

[262] *See id.* at 720 (noting that "the export regulations even contain a description of the key length in 'bits' for regulated programs").

[263] *See id.* at 720-23.

[264] *See id.* at 720-21.

[265] *See id.*

[266] *See id.* at 720 (citing Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (holding that the government's purpose is "the controlling consideration")).

[267] *Id.* at 720. Note, however, that the very nature of the software makes it difficult to separate its function from its expression. It is difficult, if not impossible, to modify source code to retain its expressive message while modifying its function to conform to export regulations. Thus, while claiming to control function, the regulations equally restrict expression. Bernstein's counsel has noted that "[t]o mandate key recovery is to mandate that computer programs have different content than they would otherwise; it's like saying that the government wants to control the 'taste' of chocolate cake rather than the recipe. Change one, you must change the other." Cohn Email, *supra* note 254.

[268] 117 S. Ct. 2329, 2344 (1997) (stating that "our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet]"). Judge Gwin also distinguished Reno v. American Civil Liberties Union by stating that encryption software, unlike pornography on the Internet, is "fundamentally and functionally different in electronic form than when in print form." *Junger*, 8 F. Supp.2d at 721.

O'Brien test.[269] The court found that all three prongs of that test were satisfied and ruled that "[b]ecause the content neutral export regulations at issue enable the government to collect vital foreign intelligence, are not directed at a source code's ideas, and do not burden more speech than necessary, they satisfy intermediate scrutiny."[270]

Having rejected all five counts raised by Junger, Judge Gwin denied summary judgment for Junger and granted summary judgment for the government.[271] Professor Junger intends to appeal Judge Gwin's decision, but until either *Junger* or *Bernstein* is reversed, a significant split between federal courts remains.[272]

IV. The Constitutional Battlefield

Much of the current debate surrounding the export of encryption software is taking place in legislative sessions as Congress looks for ways to balance the social realities of the information age with the guarantee of rights inherent in our political system. This part of the Comment discusses key constitutional issues that any export legislation must address and describes how the current regulations fare under constitutional scrutiny.[273] After the constitutional foundation is laid, the subsequent part of this Comment discusses many of the policy arguments presented by each side of the debate, including how other countries are dealing with the encryption dilemma.[274]

As seen in Part III, recent challenges to the EAR scheme cite the first, and possibly most cherished right of U.S. citizenship—freedom of expression.[275] As earlier portions of this Comment

---

[269] *See supra* notes 222-25 and accompanying text (discussing the result of *Karn*'s application of the *O'Brien* test).

[270] *Junger*, 8 F. Supp.2d at 723.

[271] *See id.* at 723-24.

[272] *See* Peter Junger, Federal District Court Holds That Software Publishers Are Not Protected by the First Amendment—Government Wins Summary Judgment in Junger v. Daley (visited Sept. 5, 1998) <http://samsara.law.cwru.edu/comp_law/jvd/pressrel-070798.txt> (press release announcing the *Junger* result and highlighting the clear split between the *Bernstein* and *Junger* courts).

[273] *See infra* notes 281-393 and accompanying text.

[274] *See infra* notes 390-468 and accompanying text.

[275] *See supra* notes 153-62, 219-25 and accompanying text.

illustrated, much of the debate centers on whether software is a protected expression.[276] Decisions in the recent encryption cases have not provided a clear answer.[277] Other constitutional arguments involve indirect infringement of rights springing from the Fourth Amendment right to privacy and the Fifth Amendment Due Process guarantees.[278] These arguments do not suggest that infringement occurs directly by restricting encryption producers' rights. Rather, they claim that encryption user rights are infringed indirectly by limiting export.[279] Although there are a number of other constitutional positions one could take,[280] this Comment focuses on the First, Fourth, and Fifth Amendment arguments that form the battlefield of most legal and legislative debates.

A. Freedom of Expression in a Programming Language

> The greater the importance of safeguarding the community from incitements to the overthrow of our institutions by force and violence, the more imperative is the need to preserve inviolate the constitutional rights of free speech, free press and free assembly . . . . Therein lies the security of the Republic, the very foundation of constitutional government.[281]

Given that computers and the Internet were unknown when the Bill of Rights was drafted, the U.S. government and its citizens are

---

[276] *See supra* notes 153-62, 167-73, 186-99, 219-28, 244-57 and accompanying text.

[277] *See* Paul Wallich, *Cracking the U.S. Code*, SCIENTIFIC AMERICAN, April, 1997, at 1 (visited Nov. 2, 1997) <http://www.sciam.com/0497issue/0497cyber.html> (reporting that California and Washington, D.C. courts have issued "diametrically opposed opinions" about the legitimacy of government controls over encryption).

[278] *See infra* notes 362-88 and accompanying text.

[279] Although relying on cherished Constitutional rights, these arguments are more complex and indirect and, thus, have not garnered the same acceptance as the First Amendment positions. *See infra* notes 362-88 and accompanying text.

[280] The restriction on electronic publication could endanger freedom of the press as guaranteed by the First Amendment. *See generally* U.S. CONST. amend. I. This freedom may also be indirectly infringed if reporters cannot use strong encryption while researching dangerous subject matter. Further, the Freedom of Assembly is endangered whenever the government requires the ability to track your correspondence. Encryption controls, and specifically the push for key-recovery, could limit association between parties who fear a government's prying eye. *See generally* U.S. CONST. amend. I.

[281] DeJonge v. Oregon, 299 U.S. 353, 365 (1937) (Hughes, C.J., writing for majority).

fighting over modern interpretation of the First Amendment which provides that "Congress shall make no law . . . abridging the freedom of speech."[282] In considering encryption software regulations, the initial First Amendment questions must be whether software is speech and, if so, whether its topic can limit the protection it is afforded. Surprisingly, *Bernstein I* was the first case to hold specifically that software was speech for First Amendment purposes.[283] This is surprising because software was accepted for copyright as early as 1964[284] and Congress confirmed that approach in 1980 by passing the Computer Software Copyright Act which categorized computer programs as copyrightable literary works.[285]

In *Bernstein I* Judge Patel did not rely on encryption software's copyrightability, but instead based her holding on the nature and properties of software.[286] In equating computer languages to spoken languages, the court relied on *Yniguez v. Arizonans for Official English*,[287] which concluded that language by its "sophisticated and complex system of understood meanings [is speech]. Language is by definition speech, and the regulation

---

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

[283] *See* Bernstein v. U.S. Dep't of State (Bernstein I), 922 F. Supp. 1426, 1434-36 (N.D. Cal. 1996).

[284] *See* FINAL REPORT OF THE NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS 15-16 (1979). This approach would be incorporated as law when Congress adopted CONTU recommendations that programs be copyrightable. *See* 17 U.S.C. §§ 101, 117 (1994); Pub. L. No. 96-517, § 10(a)-(b), 94 Stat. 3028 (1980).

[285] *See* Computer Software Copyright Act, 17 U.S.C. §§ 101, 117 (1988).

[286] *See Bernstein I*, 922 F. Supp. at 1435. Professor Junger also relied on this in noting that "[p]rograms are a medium of expression for programmers, computer scientists and anyone, like Professor Junger, 'whose ideas are described or demonstrated with the help of computer code.'" Plaintiff's Motion for Summary Judgment at 7, Junger v. Daley, 8 F. Supp.2d 708 (N.D. Ohio 1997) (No. 96 CV 1723) (visited Nov. 2, 1997) <http://www.jya.com/pdj4.htm>.

[287] 69 F.3d 920 (9th Cir. 1995) (en banc) *cert. granted*, — U.S. —, 116 S. Ct. 1316 (U.S. 1996). The case involved a constitutional challenge to the "English-only provision amended to Arizona's constitution." *Bernstein I*, 922 F. Supp. at 1435 (citing *Yniguez*, 69 F.3d at 934). The *Yniguez* defendants unsuccessfully "sought to characterize one's choice of language as expressive conduct. The court was similarly 'unpersuaded by the comparison between speaking languages other than English and burning flags.'" *Id.* (quoting *Yniguez*, 69 F.3d at 934).

of *any language* is the regulation of speech."[288] Advocates note that computer language will become even more analogous to the spoken word as future generations of automatic-programming software begin to take general programming ideas from a user and construct the necessary software.[289] With such technology, the government will be hard-pressed to argue that such general ideas are distinguishable from ordinary speech.[290]

If software is speech, the next question becomes whether the topic of that speech could limit its protection under the First Amendment. Even the spoken word is not protected for "the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words."[291] Such utterances are considered of such slight social value that any benefit derived from them is outweighed by the social interest in peace and morality.[292] Can computer "speech" be similarly limited because it discusses ideas for encryption? In *Karn* the court acknowledged the Supreme Court's view on the right to free speech as preventing "the government from proscribing speech because of disapproval of the ideas expressed."[293] To date the government has not suggested that encryption content removes software from protected expression; rather, its view has consistently been that the functional qualities of programming code allow it to be regulated as conduct.[294] This

---

[288] *Yniguez*, 69 F.3d at 934-35 (emphasis added). Building on this spoken-word equivalence, Judge Patel, in *Bernstein I*, found "no meaningful difference between computer language . . . and German or French." *Bernstein I*, 922 F. Supp. at 1435. *But see Junger*, 8 F. Supp.2d at 716 (arguing that "'[s]peech' is not protected simply because we write it in a language.").

[289] *See* Telephone Interview with Peter Junger, Plaintiff (Nov. 2, 1997).

[290] *See* Wallich, *supra* note 277, at 1.

[291] Arnold H. Loewy, *Distinguishing Speech From Conduct*, 45 MERCER L. REV. 621, 625 (1994) (quoting Chaplinsky v. New Hampshire, 315 U.S. 569, 572 (1942)). Loewy notes that such words inflict injury or tend to incite an immediate breach of the peace. *See id.* at 627-28.

[292] *See id.* at 626 (quoting *Chaplinsky*, 315 U.S. at 572).

[293] Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9-10 (D.D.C. 1996), *remanded per curiam*, 107 F.3d 923 (D.C. Cir. 1997) (quoting R.A.V. v. City of St. Paul, 505 U.S. 377, 381-82 (1992)).

[294] *See* Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,573 (1996) (to be codified at 15 C.F.R. §§ 730, 732, 734, 736, 738, 740, 742, 744, 748, 750, 768, 772, 774) (stating that "export

line of reasoning was the cornerstone of Judge Gwin's finding that "[i]n the overwhelming majority of circumstances, encryption source code is exported to transfer functions, not to communicate ideas."[295]

B. The Line Between Expression and Conduct

The government has received mixed support for its claim that the functional qualities of software limit its First Amendment protection. Although *Karn* assumed software was speech, it embraced the government's approach and applied legal doctrines particular to regulating conduct.[296] The *Bernstein* decisions, however, rejected this approach and claimed that whether programming code is functional is immaterial because "functionality of a language does not make it any less like speech."[297] Professor Junger trumpeted the dangers of regulating functional speech, noting that acknowledged expressions such as legal form books, political pamphlets, and books of sermons all have functional characteristics.[298]

The functionality question is key to understanding the proper legal standard. A facial challenge to such government regulation is applicable only where there is a "close enough nexus to expression, or to conduct commonly associated with expression, to

---

of encryption software, like export of encryption hardware, is controlled because of th[e] functional capacity to encrypt information on a computer system, and not because of any informational or theoretical value that such software may reflect, contain, or represent, or that its export may convey to others abroad.").

[295] Junger v. Daley, 8 F. Supp.2d 708, 716 (N.D. Ohio 1998).

[296] *See Karn*, 925 F. Supp. at 10.

[297] Bernstein v. U.S. Dep't of State (Bernstein I), 922 F. Supp. 1426, 1435 (N.D. Cal. 1996). Judge Patel further noted that while "instructions, do-it-yourself manuals, recipes, [and] even technical information about hydrogen bomb construction are often purely functional; they are also speech." *Id.* (citing United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wisc. 1979)).

[298] *See* Press Release, *Summary Judgment Motion Filed in Suit Attacking Restrictions on the "Export" of Software*, (Oct. 16, 1997) (visited Oct. 29, 1997) <http://samsara.law.cwru.edu/comp_law/jvd/pr_brief.txt> (noting that censorship of such expression is what led to the First Amendment). *But see Junger*, 8 F. Supp.2d at 716-18. In *Junger*, Judge Gwin rejected Professor's Junger's analogies to functional printings, relying heavily on the observation that unlike "a recipe [that] provides instructions to a cook, source code is a device . . . that actually does the function of encryption." *Id.* at 717.

pose a real and substantial threat of identified censorship risks."[299] The Supreme Court has entertained facial freedom-of-expression challenges only against statutes that "by their terms" sought to regulate words or expressive conduct.[300] The encryption export licensing scheme appears to have the required nexus; it prohibits publication without a license.[301] The more contentious and yet unresolved questions become what standard should be applied to such a licensing scheme and whether that standard has been met by the government. On this determination the *Bernstein*, *Karn*, and *Junger* courts again disagreed, and it is unclear what standard applies for encryption regulations. The following section describes the proper tests for such regulations and discusses how those tests have been applied in the encryption context.

C. Prior Restraints on Protected Expressions

Freedom of expression analysis focuses both on an expression and its regulation. Assuming there is an expression, restriction of it is governed by First Amendment principles including the doctrine of "prior restraint."[302] This doctrine has been used in two

---

[299] City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 759 (1988). *Lakewood* involved a newspaper challenge to a city ordinance requiring annual permits for newsracks on public property. *See id.* The Court contrasted laws directed at expression, such as one governing the circulation of newspapers, with laws of general applicability not aimed at conduct commonly associated with expression, such as law requiring building permits. *See id.* at 760-61.

[300] Roulette v. City of Seattle, 97 F.3d 300, 305 (9th Cir. 1996) (quoting Broadrick v. Oklahoma, 413 U.S. 601, 612-13 (1973)). At issue in *Roulette* was an ordinance that prohibited people from sitting or lying on public sidewalks in certain areas and at certain times. *See id.* The court held that "[t]he fact that sitting can possibly be expressive, however, isn't enough to sustain plaintiffs' facial challenge." *Id.*

[301] *See* Bernstein v. U.S. Dep't of State (Bernstein III), 974 F. Supp. 1288, 1305 (N.D. Cal. 1997) (noting that the scheme adversely affects scientists, programmers, and anyone working with encryption software to the extent that they cannot publish their scholarly research until removing algorithms or getting government permission).

[302] The doctrine of "prior restraint" is usually traced to the English Licensing Act of 1662, which required an official license prior to any publication. Allen M. Shinn, Jr., Note, *The First Amendment and the Export Laws: Free Speech on Scientific and Technical Matters*, 58 GEO. WASH. L. REV. 368, 382 n.89 and accompanying text (1990) (citations omitted). Blackstone provided an early view of the doctrine: "[t]he liberty of the press is indeed essential to the nature of a free state; but this consists in laying no previous restraints upon publications, and not in freedom from censure for criminal matter when published." *Id.*

distinctly different situations: "administrative licensing schemes . . . and judicially imposed injunctions."[303] The first category is most applicable to encryption regulations and has been applied to invalidate licensing schemes for pamphlets,[304] motion pictures,[305] and parades and processions.[306] The Supreme Court has noted that "prior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights . . . . If it can be said that a threat of criminal or civil sanction after publication 'chills' speech, prior restraint 'freezes' it at least for the time."[307]

This "freezing" effect of prior restraints plays a very definite role in the encryption regulation debate. A National Research Council (NRC) report commissioned by the Defense Department on cryptography policy found "that companies were reluctant to express their full dissatisfaction with the rules and implementation of [encryption] export controls."[308] They feared that "any explicit connection between critical comments and their company might result in unfavorable treatment of a future application for an export license for one of their products."[309] Lest there be any claim of unwarranted company paranoia, it is disturbing to note Admiral Bobby Inman's warning, as Deputy Director of the Central Intelligence Agency, to members of the academic community to cooperate with technology export controls or risk "far more serious threats to academic freedom."[310]

---

[303] *Id.*

[304] *See* Lovell v. Griffin, 303 U.S. 444 (1938). The Court reversed a Jehovah's Witness conviction for distributing pamphlets in violation of an ordinance requiring a permit prior to distributing "literature of any kind." *Id.* at 447.

[305] *See* Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495 (1952) (invalidating a statute requiring a license for showing motion pictures).

[306] *See* Shuttlesworth v. City of Birmingham, 394 U.S. 147 (1969) (invalidating a city ordinance forbidding parades or processions without a permit).

[307] Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976) (citation omitted).

[308] Bernstein v. U.S. Dep't of State (Bernstein III), 974 F. Supp. 1288, 1308 n.25 (N.D. Cal. 1997) (citing National Research Council (NRC), National Academy of Sciences, *Cryptograph's* [sic] *Role in Securing the Information Society* C-2 (prepublication copy May 30, 1996)).

[309] *Id.* (quoting NRC Report at 4-29).

[310] Gina Kolata, *CIA Director Warns Scientists*, 215 SCIENCE 383 (1982).

1. The Many Tests for Prior Restraints

While the Supreme Court has never embraced *per se* invalidity of prior restraints,[311] "[a]ny system of prior restraints of expression comes to [the] Court with a heavy presumption against its constitutional validity."[312] For any scheme to meet this presumption, the government has the burden of justifying the restraint, but the exact standard it must meet is unclear. There are at least four tests involved in this determination, but their interrelation is complex.[313] The following understanding of the tests appears to be most consistent with federal court uses.

a. Why the Restraint?

The first determination involves whether the regulations are content-neutral or content-based. In other words, does the restraint limit expression specifically because of its content or incidentally as part of implementing a content-neutral scheme?[314] Content-based regulations warrant strict scrutiny and are generally held to be unconstitutional.[315] Although content-neutral regulations are subject to a lesser degree of scrutiny, the standard constitutional ends-means analysis has not been consistently applied. Instead, different analyses are applied depending on whether expression or conduct is regulated.

b. The O'Brien *Test for Regulating Conduct*

In the case of content-neutral regulations of conduct, a four-

---

[311] *See* New York Times Co. v. United States, 403 U.S. 713, 731 (1971) (per curiam) (White, J., concurring); *see also* Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971).

[312] *New York Times Co.*, 403 U.S. at 714 (quoting Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963) (citations omitted)). *New York Times*, better known as the *Pentagon Papers* case, involved the publishing of sensitive military documents during the Vietnam War. *See id.*

[313] In fact, commentator Geoffrey R. Stone found at least seven seemingly different standards for content-neutral review. *See* Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 48-54 (1987).

[314] *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 383-87 (1992).

[315] *See* Jill M. Ryan, Note, *Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption*, 4 WM. & MARY BILL RTS. J. 1165, 1200 (1996).

pronged test similar to the ends-means analysis was established in *United States v. O'Brien*.[316] Referred to as the *O'Brien* test, it was applied in upholding the government prohibition against burning draft cards.[317] The test questions whether the regulation is within the constitutional power of the government, furthers an important or substantial government interest, is unrelated to the suppression of free expression, and the incidental restriction on speech is no greater than is essential to further the governmental interest.[318]

c. *The* Freedman *Test for Regulating Expression*

Regarding content-neutral regulations of expression, a more stringent test has been applied in addition to heightened scrutiny. Unlike the *O'Brien* test, which focuses on authority to regulate, the test applied in *Freedman v. Maryland*[319] focuses on the procedural safeguards inherent in the regulations.[320] The Court recognized the danger inherent in prior restraints, as a government official, rather than a judicial process, holds the delicate responsibility of regulating the permissibility of speech.[321] The Court outlined three procedural safeguards that comprise the *Freedman* test: (1) any restraint prior to judicial review can be imposed only for a brief and specified period during which the status quo prevails; (2) expeditious judicial review must be available; and (3) the censor must bear the burden of going to court to suppress speech and, once there, bears the burden of proof.[322] In addition to these three considerations, the Court has, at different times, imposed two other requirements, namely the

---

316 391 U.S. 367 (1968).

317 *See id.*; *see also supra* notes 155-56 (describing the *O'Brien* test).

318 *See id.* at 377. The "narrowly tailored" test can also be seen as two separate tests involving whether (1) the government interest is unrelated to the suppression of free expression and (2) the incidental restriction on speech is no greater than is essential to further that interest. *See id.*

319 380 U.S. 51 (1965).

320 *See id.*

321 *See id.* at 58 (holding that "a noncriminal process which requires the prior submission of a film to a censor avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system").

322 *See* FW/PBS, Inc. v. Dallas, 493 U.S. 215, 227 (1990) (citing Freedman v. Maryland, 380 U.S. 51, 58-60 (1965)).

restraint must impose "narrow, objective and definite standards to limit the discretion of the licensing officials,"[323] and the government must establish a threat of "direct, immediate and irreparable harm."[324]

2. *Application to Encryption Export Licensing*

Although applying the above tests to encryption regulations may appear straightforward, the courts have shown otherwise. The *Bernstein III* court disagreed with the *Karn* and *Junger* courts on each of the major determinations. As an initial matter, only the *Bernstein III* court referred to the restrictions as prior restraints and thus acknowledged a presumption of invalidity.[325] All three courts agreed, however, that the regulations involved were content-neutral.[326] The analysis in *Bernstein III* diverged from the approaches adopted in *Karn* and *Junger* on considering whether expression or conduct was regulated. The *Bernstein III* court focused on the expression inherent in encryption software and applied the stringent *Freedman* factors.[327] The *Karn* court accepted the government's argument that export conduct was the regulation focus and thus considered *O'Brien* to be the proper test.[328] The *Junger* court short-circuited the entire prior restraint analysis by declaring that "encryption software is not typically expression, [and thus] a facial challenge does not succeed."[329]

---

[323] Forsyth County v. The Nationalist Movement, 505 U.S. 123, 131 (1992) (quoting Shuttlesworth v. Birmingham, 394 U.S. 147, 150-51 (1969)).

[324] New York Times Co. v. United States, 403 U.S. 713, 730 (1971) (per curiam) (Stewart, J., concurring).

[325] *See* Bernstein v. U.S. Dep't of State (Bernstein III), 974 F. Supp. 1288, 1304 (N.D. Cal. 1997) (noting that prior restraints begin with a presumption of invalidity).

[326] *See id.* at 1307; Karn v. U.S. Dep't of State, 925 F. Supp. 1, 10 (D.D.C. 1996), *remanded per curiam*, 107 F.3d 923 (D.C. Cir. 1997); Junger v. Daley, 8 F. Supp.2d 708, 720-21 (N.D. Ohio 1998). Note that the restrictions actually appear content-based because they focus on encryption content. Nevertheless, Judge Patel applied content-neutral review and ruled that the regulations failed even that lighter standard. *See Bernstein III*, 974 F. Supp. at 1307-08.

[327] *See Bernstein III*, 974 F. Supp. at 1307-08.

[328] *See Karn*, 925 F. Supp. at 10-11.

[329] *Junger*, 8 F. Supp.2d at 718 (N.D. Ohio 1998) (noting that "[e]ven if the Export Regulations have impaired the isolated expressive acts of academics like Plaintiff Junger, exporting software is typically non-expressive.").

Before applying the *Freedman* factors, the *Bernstein III* court considered the government interest involved.[330] The claimed, and likely actual, end to be served by encryption regulations was national security.[331] This interest carries substantial weight in constitutional analysis. However, national security *alone* has been deemed too amorphous a rationale to abrogate the protections of the First Amendment.[332] Although not specifically mentioned in the analysis, the test for "direct and irreparable harm" is closely tied to the national security issues considered.[333] In fact, the *Bernstein III* result may have been different if direct and irreparable harm had been at issue.[334]

Turning to the first of the *Freedman* factors, the court considered whether the regulations require licensing decisions within a specific and reasonable period of time.[335] Although export applications are resolved or referred to the President within ninety days,[336] there is no time limit placed on an application once referred to the President.[337] Even the appeals process only required decisions "within a reasonable time after receipt of the appeal."[338] The second factor, which requires prompt judicial review, further leaves the regulations infirm because it considers agency decisions

---

330 *See Bernstein III*, 974 F. Supp. at 1307.

331 *See id.*

332 *See* New York Times Co. v. United States, 403 U.S. 713, 723 (1971) (per curiam) (Douglas, J., concurring) (stating that Near v. Minnesota *ex rel.* Olson, 283 U.S. 697 (1931) repudiated an absolute security interest in no uncertain terms).

333 *See id.*

334 With regard to encryption export, the government has never claimed direct and irreparable harm; rather, security arguments rely on rationale generally reserved for "secondary effects." The "secondary effects" doctrine considers the harm caused after viewing a restricted expression (for example, pornographic movies instigating sex crimes). *See* Renton v. Playtime Theaters, Inc., 475 U.S. 41 (1986). The secondary effects rationale has never been extended beyond sexually explicit speech. *See* Boos v. Barry, 485 U.S. 312 (1988) (refusing to apply the rationale to political speech); *see also* Reno v. American Civil Liberties Union, 117 S. Ct. 2329 (1997) (considering the secondary effects doctrine in relation to a statute regulating speech on the Internet).

335 *See Bernstein III*, 974 F. Supp. at 1308.

336 *See* 15 C.F.R. § 750.4(a) (1998).

337 *See Bernstein III*, 974 F. Supp. at 1308.

338 15 C.F.R. § 756.2(c)(1) (1998).

to be final and not subject to judicial review.[339] This restriction also caused the regulations to fail the last *Freedman* factor, which requires a licensor to either issue a license or go to court to seek a restraint.[340] The *Bernstein III* court also found the regulations to be "lacking . . . any standards for deciding an application"[341] because the EAR requires application review on a "case-by-case basis" and appears to impose no limits on agency discretion.[342] In summary, Judge Patel remained true to her *Bernstein II* opinion, which labeled the scheme a "paradigm of standardless discretion."[343]

The *Karn* analysis applied the less stringent standard for content-neutral conduct regulation and, not surprisingly, reached the opposite result.[344] Both the first and second *O'Brien* prongs were satisfied because the plaintiff did not dispute them.[345] Although the first prong (regulating export was within the constitutional power of government), was difficult to debate, it is somewhat surprising that the government interest was not disputed. In the face of no rebuttal, the government convinced the court that "interception of communication made by foreign intelligence targets is 'essential to the national defense, national security, and the conduct of the foreign affairs of the United States.'"[346] The plaintiff instead focused on the third prong, which required that "incidental restriction on alleged First Amendment freedoms [be] no greater than is essential to the furtherance of [the government's] interest."[347] The plaintiff argued that his algorithms "were already widely available in other countries . . . or [were] so 'weak' that they could be broken by the [National Security

---

339 *See id.* at § 756.2(c)(2).

340 *See* Freedman v. Maryland, 380 U.S. 51, 58-59 (1965).

341 *Bernstein III*, 974 F. Supp. at 1308.

342 15 C.F.R. § 742.15(b) (1998).

343 Bernstein v. U.S. Dep't. of State (Bernstein II), 945 F. Supp. 1279, 1289 (1996). Although Judge Patel's strong remarks dealt with ITAR, her EAR decision found similar problems. *See Bernstein III*, 974 F. Supp. at 1308.

344 *See* Karn v. U.S. Dep't of State, 925 F. Supp. 1, 10 (D.D.C. 1996), *remanded per curiam*, 107 F.3d 923 (D.C. Cir. 1997).

345 *See id.* at 11.

346 *Id.* (citation omitted).

347 *Id.* (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968)).

Agency]," but the court considered this to be a second-prong argument.[348] Further, the court considered the argument to be a policy dispute with the President "for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry."[349] Thus what began as an *O'Brien* analysis came to center on separation of powers concerns. Requests by the plaintiff to balance First Amendment harms with any injury to national security were also rebuffed by Judge Richey.[350] The final *Karn* result left the export restrictions intact, but the prior restraint arguments by the plaintiff and the analysis by the court appear insufficient in the face of *Bernstein*'s exhaustive analyses.

The *Junger* analysis applied neither the *Freedman* nor the *O'Brien* test. Rather, Judge Gwin began with the proposition that publishing encryption source code was conduct and went on to apply conduct-specific rules to reject Junger's prior restraint assertion.[351] The conduct case, *Roulette v. City of Seattle*,[352] was pivotal in Judge Gwin's finding that "the prior restraint doctrine is not implicated simply because an activity may on occasion be expressive."[353] Based on this finding, the court was able to reject the facial challenge without even considering the adequacy of the regulation's procedural safeguards.[354]

---

[348] *Id.* (citation omitted) (second alteration in original).

[349] *Id.* at 11-12 (quoting Chicago & Southern Airlines v. Waterman SS Corp., 333 U.S. 103, 111 (1948)).

[350] *See id.* at 12 (stating again that scrutiny into actual injury of national security is a political question not subject to review).

[351] Junger v. Daley, 8 F. Supp.2d 708, 718-19 (N.D. Ohio 1998).

[352] 97 F.3d 300 (9th Cir. 1996) (holding that although sitting on city sidewalks may occassionally be expressive, city ordinance prohibiting sitting is not subject to facial challenge).

[353] *Junger*, 8 F. Supp.2d at 718. Although this appears to supply a short and simple answer to the prior restraint conflict between *Bernstein III* and *Karn*, the court's assumption that the publication of source code by Junger or other cryptographers constitutes conduct is flawed. Claims that source code is rarely expressive demonstrates the technological ignorance of the courts. In fact, a critical component of trusted encryption algorithms is that they have been published and subjected to critical review. *See supra* notes 66-67 and accompanying text.

[354] *See Junger*, 8 F. Supp.2d at 719.

D. Other Constitutional Avenues

Although this Comment is not intended to provide in-depth analysis of all constitutional issues relating to encryption export, it is worth noting a few other constitutional arguments that could be developed in litigation or commentary. These additional issues include overbreadth, and Fourth and Fifth Amendment infirmities of the current encryption export scheme.

1. The Overbreadth Doctrine

Overbreadth as a constitutional doctrine allows a person whose own speech is protected to challenge an overbroad law on its face to protect his own speech,[355] as well as the speech of others not before the court.[356] The challenge is aimed at a regulation that "does not aim specifically at evils within the allowable area of state control but . . . sweeps within its ambit other activities protected" by the First Amendment.[357] Regarding the encryption export scheme, *Junger* argued it "covers encryption software after it is already available overseas and on the Internet, interferes with academic freedom, and restricts rights to communicate not just with foreign persons outside the United States, but with United States citizens."[358] Further, it may even reach software that contains no encryption capability whatsoever under provisions regulating encryption software.[359] In addition, *Junger*'s overbreadth challenge was impacted by the requirement that "a plaintiff must show that the law will have a significant and different impact on third parties' free speech interests than it has

---

[355] *See* Board of Trustees of S.U.N.Y. v. Fox, 492 U.S. 469, 484 (1989).

[356] *See* Forsyth County v. National Movement, 505 U.S. 123, 129 (1992).

[357] Thornhill v. Alabama, 310 U.S. 88, 97 (1940). Such a threat "must not only be real, but substantial." Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973).

[358] Plaintiff's Motion for Summary Judgment at 15, Junger v. Daley, 8 F. Supp.2d 708 (N.D. Ohio 1998) (No. 96 CV 1723) (visited Nov. 2, 1997) <http://www.jya.com/pdj4.htm>.

[359] *See id.* Such products include word processors and communications software that allow "plug-in" encryption modules. *See* Telephone Interview with Peter Junger, Plaintiff (Nov. 2, 1997). Although the products are not shipped with encryption capability, their interface designed to use encryption "plug-ins" could bring them under export scrutiny. *See id.*

on his own."[360] Although no court has invalidated an encryption regulation on this logic, that is likely because the overbreadth doctrine is "concededly 'strong medicine' employed as a last resort when a limiting construction cannot be applied to a statute."[361]

2. *The Fourth Amendment: Right to Privacy*

The Fourth Amendment to the Constitution states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[362] This right has become commonly known as the right to privacy, and such a claim begins with establishing two elements: (1) that State action is at issue[363] and (2) that there is a reasonable expectation of privacy in the compromised communication.[364] Once these elements have been met, the inquiry turns to balancing individual privacy interests against the government's interest in breaching that privacy.[365]

The typical violation of privacy is a warrantless police search;

---

[360] Junger v. Daley, 8 F. Supp.2d 708, 719 (N.D. Ohio 1998) (citing members of City Council of City of Los Angeles v. Taxpayers for Vincent, 466 U.S. 789, 801 (1984)). Although Judge Gwin applied this critical element of overbreadth analysis, it appears he unnecessarily restricted his focus to "other academics" rather than including anyone wishing to electronically publish encryption source code. *Id.*

[361] Bernstein v. U.S. Dep't of State (Bernstein I), 922 F. Supp. 1426, 1438 (N.D. Cal. 1996) (citing Broadrick v. Oklahoma, 413 U.S. 601, 613, (1973)). In fact, the "strong medicine" view of overbreadth challenges was directly referenced in *Junger*. *See Junger*, 8 F. Supp.2d at 719.

[362] U.S. CONST. amend IV. The Amendment further states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

[363] *See* Lennon, *supra* note 18, at 479-80.

[364] *See id.* This involves a recent interpretation of the Fourth Amendment that is broader than that applied for most of its history. Traditional interpretation placed great emphasis on words such as "persons, houses, papers, or effects" to the point that wiretaps had no Fourth Amendment implications. *See id.* at 481 nn. 97-99. The Warren Court originated the modern, more adaptive application. *See id.* at 481 n.99.

[365] *See* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624 (1989) (noting that searches without "individualized suspicion" are allowed "in limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion").

however, modern Fourth Amendment interpretation encompasses a "legislative search" by passage of laws limiting citizen privacy.[366] Where such law or rulemaking is done by an agency or organization, finding State action may require a complex analysis of funding and control issues. However, regarding encryption regulations, commentators have noted "the method by which one's encoding ability would be controlled would be legislative—the epitome of unequivocal state action."[367] The next question involves the reasonable expectation of privacy in electronic communications, and again, legislative actions dictate the analysis. In particular, the Electronic Communications Privacy Act of 1986[368] provides a clear indication of society's on-line privacy expectations by forbidding unauthorized interception of email, inter-computer communications, and cellular phone transmissions.[369]

The final and most difficult analysis involves balancing privacy and governmental interests. Where government searches are focused on a particular investigative target, *Winston v. Lee*[370] represents the typical approach, comparing the "great" state interest in policing a crime to individual interests in privacy.[371] However, given that encryption restrictions are not predicated upon a particularized suspicion, a tougher *Skinner v. Railway Labor Executives' Association*[372] balancing test is applied. In that case the Court held that broad, targetless searches are allowable only "where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered

---

366 *See* Lennon, *supra* note 18, at 480-81.

367 *Id.* at 480 (citing William B. Harvey, *Private Restraint of Expressive Freedom: A Post-Prune Yard Assessment*, 69 B.U. L. REV. 929, 969 (1989)).

368 18 U.S.C. §§ 2510-2711 (1988).

369 *See* Manufacturas Int'l, Ltd. v. Manufacturers Hanover Trust Co., 792 F. Supp 180 (E.D.N.Y. 1992) (protecting computer transmissions from electronic eavesdropping). For a listing of wiretap cases see *Lennon*, *supra* note 18, at 483-84 n.113. Note however that the mobility of pagers and personal digital assistants may limit the expectation of privacy of such devices. *See* Lennon, *supra* note 18, at 486-87.

370 470 U.S. 753 (1985).

371 *See id.* (balancing the government and personal interests involved in removing a bullet from a person's body to aid law enforcement).

372 489 U.S. 602 (1989).

by the intrusion would be placed in jeopardy by a requirement of individualized suspicion."[373] Although particular wiretapping successes, such as capturing child molesters appear, in hindsight, to evidence the government's important interest in eavesdropping, there is little to suggest that handicapping everyone's encryption abilities is necessary for those successes.[374] The resulting governmental interest appears lacking in comparison to the citizenry's interest in free and private exchange of ideas. As on-line communications make up a larger portion of daily discourse, this privacy interest will only grow. The importance will not lie in an individual paper or personal effect, but will involve the very lifeline of societal interconnectedness.

3. The Fifth Amendment: Substantive Due Process for Fundamental Rights

An intimately related constitutional argument involves the Fifth Amendment, which guarantees that no person shall be "deprived of life, liberty, or property, without due process of law."[375] From those vanilla words has sprung the controversial doctrine of substantive due process, which requires strict scrutiny for laws affecting fundamental rights.[376] This approach is intertwined with Fourth Amendment analysis because privacy is again the key issue. Although courts have recognized a fundamental right in various privacy-related topics such as abortion[377] and right-to-die decisions,[378] the general right to private communications has not been established. The broad test for

---

[373] *Id.* at 624.

[374] Commentators have noted that only 183 wiretaps have been affected by encryption. *See* Lennon, *supra* note 18, at 494 (citing statistics presented by FBI Director Louis Freeh); *see Cost of Wiretap Bill Examined at House Subcommittee Hearing*, Daily Rep. for Executives (BNA) No. 176, at A13, A14 (Sept. 14, 1994). Given that between 1982 and 1991 alone, over 7,467 wiretaps were conducted, commentators question the significance of any law enforcement impact. *See id.*

[375] U.S. CONST. amend. V.

[376] *See* GEOFFREY R. STONE ET AL., CONSTITUTIONAL LAW 813-42, 940-1072 (3d ed. 1996) (describing both the early fundamental right to contract and modern substantive due process rights such as privacy, personhood and family).

[377] *See* Roe v. Wade, 410 U.S. 113 (1973).

[378] *See* Cruzan v. Director, Missouri Dep't of Health, 497 U.S. 261 (1990).

establishing such a right requires looking to the "traditions and [collective] conscience of our people."[379] The test involves whether the right in question "cannot be denied without violating those 'fundamental principles of liberty and justice which lie at the base of all our civil and political institutions.'"[380]

Historic evidence supports both sides of the encryption debate because the forefathers have a history of encrypting messages,[381] but they also have a history of intercepting and monitoring private communications.[382] To accurately apply fundamental rights principles, the debate may need to focus on whether unbreakable encryption[383] is the issue. Throughout history the government has typically been more cryptographically advanced than its citizens and, thus, tradition may teach that private citizens have a fundamental right only in breakable encryption. Only in the last ten years has private computing power enabled individuals to utilize encryption algorithms which significantly limit government access. Unfortunately, this technology phenomenon limits the "traditions" fundamental rights analysis and may force more esoteric discussions of Bill of Rights "penumbras"[384] creating a right to privacy.

---

[379] Griswold v. Connecticut, 381 U.S. 479, 493 (1965) (Goldberg, J., concurring) (internal citations omitted).

[380] *Id.*

[381] *See supra* note 59 and accompanying text (discussing early use of encryption by James Madison and Thomas Jefferson).

[382] *See The Impact on America's Software Industry of Current U.S. Government Munitions Export Controls: Hearings Before the Subcomm. on Economic Policy, Trade and Environment of the House Comm. on Foreign Affairs*, 103d Cong., 5 (1993) (statement of Stephen T. Walker, President, Trusted Information Systems, Inc.) (noting that the ability of the U.S. government to obtain information on its adversaries has been vital to U.S. security for many years).

[383] By unbreakable the author means encryption which current governmental technologies are not able to break in a police-acceptable time period. Some commentators suggest that the government confuses the concept of making wiretapping "more difficult" with the notion of making it impossible. *See* Mike Godwin, *To Tap or Not To Tap*, COMM. ACM, Mar. 1993, at 34.

[384] *See Griswold*, 381 U.S. 479 at 484 (finding a right to privacy in the "penumbra" of many privacy-related rights protected in the Constitution).

4. A Final Constitutional Note: Whose Rights are at Stake

As mentioned above, there are a number of constitutional approaches to the encryption battle, and this Comment focused on First, Fourth, and Fifth Amendment concerns. It is important to note that these arguments do not all protect the same victim. The First Amendment issues pertain to software providers and their freedom of expression in their code. That is, the regulations form a prior restraint and force encryption code publishers to obtain a license before they can publish their encryption solutions to the rest of the world.[385] These victims appear to receive the most favorable treatment in the courts, possibly because their injury is easy to see and remedy.

However, the Fourth and Fifth Amendment arguments present an entirely different victim and a couple of levels of indirection that limit their persuasiveness. These arguments attempt to protect encryption users—conceivably everyone—in their desire to communicate privately.[386] This group is rather nebulous and it may be difficult for courts to pinpoint a common right due to such a diverse group. Further, the regulations at issue affect these victims only indirectly. The courts are asked to accept that removing regulations on one group, publishers, will remedy a violation experienced by a different group, users. An even greater leap is necessary because encryption regulations are focused on export only. The courts are asked to accept that, for economic

---

[385] *See generally supra* notes 302-10 and accompanying text (describing the application of the prior restraint doctrine to licensing schemes).

[386] Justice Douglas summarized the fear underlying these arguments in stating:

> The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears . . . . If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.

Osborn v. United States, 385 U.S. 323, 353-54 (1966).

reasons, providers will not invest in creating two versions of their product, domestic and international.[387] Domestic users thus will receive the lowest common denominator of encryption technologies.[388]

V. Encryption Policies Both Home and Abroad

Although the constitutional arguments outlined above encompass the majority of encryption issues discussed in the courts, it is also important to understand the policy considerations of the recent private encryption debate. Further, while U.S. legal doctrines may be interesting for international entities, true insights grow from the common encryption policy concerns that all governments face. This section focuses on outlining these policy concerns and concludes by surveying the international and domestic regulatory activities taking place to address these concerns.

A. The Metes and Bounds of the Encryption Policy Debate

Before discussing each of the major encryption issues, it is important at the start to recognize a few encryption regulation alternatives that form the battlefield. Key management, as briefly discussed in Part II,[389] plays a large role in international and legislative debates. The question of whether governments should require key recovery, which is essentially giving individuals or law enforcement a "spare key" to decrypt private conversations,[390] is not an easy one in light of the personal and national security interests being balanced. The regulatory alternatives in this balance can be grouped in four categories: (1) regulations

---

[387] *See* Elizabeth Corcoran, *Who Will Hold the Key? Two Bills Reflect the Split Over Restrictions*, at F15 (visited Jan. 31, 1998) <http://www.washingtonpost.com/wp-srv/tech/analysis/encryption/issues.htm>. The author cites industry executive concerns that export restrictions affect what is sold here because companies find it costly to offer separate products in different markets. *See id.* This creates an industry tendency to sell simpler, exportable products both within the United States and abroad. *See id.*

[388] *See* Johnson, *supra* note 75, § 5.3 (noting that "export controls on encryption software discourage distribution of strong encryption software" in the United States).

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

[390] *See* Corcoran, at F15 (referring to two competing bills which differ on whether law enforcement agencies should have "spare keys" to unlock scrambled information).

prohibiting use of strong encryption as defined by the government; (2) regulations allowing use of strong encryption only if government key recovery exists for law enforcement benefit; (3) regulations allowing use of strong encryption only if private key recovery exists for private data recovery benefit; or (4) regulations allowing use of strong encryption with no key recovery requirements.[391]

In addition to key recovery alternatives, governments must decide whether encryption restrictions should focus on domestic use or international export. While the majority of U.S. encryption regulation attempts have focused on export controls, the past year has seen an increased push by law enforcement for limiting domestic encryption use.[392] This recent domestic focus is having two effects: (1) resources focused on fighting export regulations have been shifted to opposing this new and greater threat to personal liberties, and (2) as regulation hits closer to home, legislators and their constituencies are taking notice of the "Big Brother" ramifications and fighting harder against all encryption regulations.[393] Although the government has consistently insisted that there are serious national security concerns, several regulation criticisms have been advanced.

1. The Cornerstone Government Argument: National Security

As mentioned in the constitutional analysis above, the underlying government objective in encryption regulations is to maximize national security.[394] Because such a foreign affairs topic

---

[391] This fourth alternative is essentially a government statement that they trust the market system to produce the most efficient result. Such a solution would require little legislation—possibly involving statutes aimed at pre-empting intrusive state law enforcement encryption restrictions.

[392] *See* Alex Lash, *FBI wants domestic crypto keys*, (visited Oct. 3, 1998) <http://www.news.com/News/Item/0,4,12317,00.html>.

[393] *See* Courtney Macavinta, *Group to attack Clinton on crypto*, (visited Oct. 3, 1998) <http://www.news.com/News/Item/0,4,19388,00.html>.

[394] The FBI has argued that widespread availability of strong encryption makes it difficult if not impossible for government agencies to effectively use wiretaps against criminals, drug dealers, and terrorists. *See* Pilkington, *supra* note 19, at 164-65 n.43 and accompanying text.

is traditionally non-justiciable, the government has been forced to provide more justifications to the public for this stance than to the courts. In short, law enforcement feels that the spread of encryption software would "help spies, terrorists and other 'enemies' of America keep communications secret from NSA's electronic eavesdroppers."[395] The FBI has stated that the results of widespread encryption could include "increase in loss of life, attributable to an inability to prevent terrorist acts and murders, an increase in corruption and in the availability of illegal drugs, and a substantial increase in undetected and unprosecuted violent crimes."[396] These possibilities stem from both an inability to crack strong encryption, and a difficulty in identifying criminal activity.[397] Regulations that encourage law-abiding citizens to use weak encryption allow law enforcement to look only for those communications using strong encryption.[398] Thus, unregulated encryption use would create a flood of data streams that all look alike, and law enforcement would have to resort to off-line means for identifying criminal communications.

Direct criticisms of the government's argument are: (1) the majority of law enforcement currently does and will always require non-decryption methods of investigation and (2) limiting encryption levels or forcing key recovery is actually more dangerous for national security than the alternative.[399] Regarding

---

[395] Evans, *supra* note 5, at 487 (citations omitted).

[396] Pilkington, *supra* note 19, at 164-65 n.43.

[397] *See* Evans, *supra* note 5, at 487-88 & n.222 and accompanying text (noting that it becomes much more difficult for the NSA to find criminal communications as more and more information is encrypted).

[398] This has mainly been discussed by commentators and opponents. *See generally id.* It would be difficult for law enforcement to discuss any eavesdropping tactics which focus on encryption use rather than criminal probable cause.

[399] "The U.S. Commerce Department has reported that 'new technologies are the strongest assurance for maintaining a superior national security posture.'" Evans, *supra* note 5, at 488-89 (quoting Gary K. Bertsch & Steven Elliot-Gower, *U.S. Export Controls in Transition: Implications of the New Security Environment*, TECH. MARKETS AND EXPORT CONTROLS IN THE 1990S 105, 111 (1991)). Technologists have also noted that security is not served by encryption regulations because they are not feasible. *See Security Hearings*, *supra* note 30, at 23 (statement of Rep. Bob Goodlatte) (noting that "people who are bound to use encryption to try to commit crimes are not going to escrow their keys."); *see id.* at 91 (statement of Matthew Blaze, principal research

non-decryption methods, Philip Karn disputed a law enforcement charge that Aldrich Ames thwarted investigations by using encryption.[400] In fact, Karn said that Ames was "easily convicted on the basis of other overwhelming evidence . . . from microphones physically planted in his house that picked up many incriminating telephone conversations."[401] Further, such traditional law enforcement techniques would work even if criminals used unbreakable encryption for their communications.[402] Regarding the danger of regulating encryption, commentators have noted that discouraged technologies will not receive research and development dollars.[403] This leads to national atrophy in that technology as other, non-regulating countries move ahead.[404] The ultimate result of this cycle for encryption is that other countries and their citizens will be able to communicate using technologies U.S. law enforcement are unable to break. Even worse, the United States and its citizens will communicate with technologies inferior to those of the criminals of the world, leaving the United States vulnerable to commercial and military attacks.[405] This reasoning is the basis for a litany of encryption regulation criticisms on behalf of consumers.

---

scientist, AT&T Research) (warning that comprehensive key escrow entails great complexity with inevitable failures); *see* Abelson et al., *supra* note 33 (noting that the technology infrastructure required for today's key recovery solutions is enormously complex and is far beyond the experience and current competency of the field).

[400] *See* Philip R. Karn, Jr., *Before the House Judiciary Committee Subcommittee on Courts and Intellectual Property Additional Comments of Philip R. Karn, Jr.*, March 20, 1997 (visited Jan. 31, 1998) <http://people.qualcomm.com/karn/export/followup.html> (questioning claims by the government that Aldrich Ames was able to thwart law enforcement efforts by using encryption methods).

[401] *Id.*

[402] *See id.*

[403] *See* Johnson, *supra* note 75, § 3.9 (noting that "when a technology is discouraged by over-regulation, taxation or other means, that technology becomes less profitable in the country where it is discouraged.").

[404] *See id.*

[405] *See* Sen. Patrick Leahy, chief sponsor of The Encrypted Communications Privacy Act, S.376, *Encryption: The Best On-line Crime Prevention Tool*, *passim* (July 28, 1997) (visited Jan. 31, 1998) <http://www.senate.gov/~leahy/s970728.html> (noting that "[t]he best defense for computer break-ins—both accidental and intentional—is a good offense").

2. Consumer Protection and Privacy

Although mechanically the same, arguments about weakening consumer encryption stand on two different grounds: (1) consumers are best protected from criminals by strong encryption and (2) consumers are best protected from the government by strong encryption.[406] The focus on criminal activity relies on market discussions of how best to expand the Internet and world economies. The focus on government intrusion relies on human rights discussions of whether citizens should be allowed to communicate privately.[407]

As technology expands and accelerates channels of communication, consumer vulnerability also increases.[408] Encryption provides many the opportunity to gain the benefits of powerful information technologies while minimizing vulnerability. As noted by cryptography expert Michael Johnson, "[n]o law can keep spies and criminals from listening to [our communications], . . . but encryption can make . . . [such communications] unintelligible to criminals and other unauthorized listeners."[409] Key recovery plans in particular have been cited as increasing vulnerability.[410] Mandatory key recovery infrastructures, which place thousands of keys in one location,[411] will "create extremely valuable targets, more likely to be worth the

---

[406] Although strong encryption is often referred to as encryption with keys longer than 56 bits, the use of the term in this section also assumes no key recovery is involved that might jeopardize security.

[407] *See also supra* notes 375-84 and accompanying text (discussing the constitutional arguments for a right to privacy). This short discussion focuses on the policy arguments being made by individuals, rather than legal doctrines. Understanding the policy arguments is essential to analyzing international encryption solutions since national privacy laws differ dramatically.

[408] *See* Abelson et al., *supra* note 33, § 1.1 (noting that "[t]he basic communication infrastructure of our society is becoming less secure, even as we use it for increasingly vital purposes").

[409] Johnson, *supra* note 75, § 3.7.

[410] *See* Abelson et al., *supra* note 33, § 3.1.3.

[411] Such key recovery agents play a vital role in all government key recovery solutions. These agents manage thousands of keys and provide access for law enforcement agencies or individuals—or lose their key. *See* Abelson et al., *supra* note 33, § 3.1.3.

cost and risk of attack."[412] As increasingly private data such as banking and medical records travel online, the protection limitations mandated by encryption regulation cause greater concern for consumers.

In addition to the issue of vulnerability to criminal intrusion, weak or key recovery encryption leaves citizens at the mercy of their government's commitment to privacy. While most privacy arguments turn immediately to the U.S. Constitution and its Fourth Amendment, it is important to remember that not all countries recognize that protection. Phil Zimmerman has learned of this disparity first-hand through communications such as one from Latvia stating: "If dictatorship takes over Russia your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks."[413] As interactions become more global it won't matter whether one's home country values privacy. Communications which bounce across the Internet will undoubtedly pass through countries with a different threshold of privacy respect.[414] In fact, commentators have suggested that "[n]ational law enforcement agencies . . . might abuse their key recovery authority to the advantage of their own country's corporations."[415]

3. Economic Impacts

The final criticism of encryption export controls is the one that garners the most attention in social and legislative circles, namely

---

[412] *Id.*

[413] William M. Bulkeley, *Cipher Probe: Popularity Overseas of Encryption Code Has the U.S. Worried*, WALL ST. J., Apr. 28, 1994, at A1; *see also Security Hearings*, *supra* note 30 (statement of Phillip Zimmerman, Chairman and Chief Technology Officer, Pretty Good Privacy, Inc.) (recalling thankful email from Burmese parents that don't understand our "fascination with such a narrow, rare, crime as [child pornography] . . . because over there . . . they're concerned about children there too, not so much for child pornography, but because in that part of the world children are tortured in front of their parents, to extract confessions").

[414] *See id.* at 74 (statement of Jerry Berman, Executive Director, Center for Democracy and Technology) (noting that "[t]he Fourth Amendment, which is a wonderful embodiment of our Constitution, does not apply to the world").

[415] Abelson et al., *supra* note 33, § 3.1.2.

that encryption controls hurt domestic companies.[416] The criticism is not hollow commercial banter; rather, a joint study by the NSA and the Commerce Department on the effect of export controls concluded that "[e]ncryption controls are harming United States firms."[417] The financial harm to the American computer industry is estimated to reach sixty billion dollars annually by the year 2000.[418] The losses affect not only email encryption providers such as PGP, but also mass-market software firms such as Microsoft and IBM.[419] Baltimore Technologies, a Belgium-based security software company, is winning customers abroad and has found that their banking customers "didn't even consider any U.S. cryptography vendor because [they] needed full 128-bit encryption."[420] A true measure of the impact is likely larger than reported because companies fear that expressing dissatisfaction could hinder their future export licensing requests.[421] Nevertheless, this dampening effect may be disappearing as more firms join the push for encryption export reform. Indeed, as firms and citizens across the world recognize the many issues involved, national legislative forums serve as precursors to an impending international resolution.[422]

---

[416] *See* Pilkington, *supra* note 19, at 163-64 (noting that there is widespread agreement that "export controls on encryption hamper United States competitiveness and cause United States firms to lose worldwide market share for mass marketed software, an industry which United States firms previously dominated") (citations omitted).

[417] *Id.* at 164.

[418] *See Security Hearings*, *supra* note 30, at 126 (statement of Jerry Berman, Executive Director, Center for Democracy and Technology, regarding a survey of 13 large American technology firm CEOs).

[419] *See* Evans, *supra* note 5, at 481 n.150 (noting Wordperfect Corporation's claims that it would have used a stronger encryption algorithm if export regulations permitted).

[420] Niall McKay, *128-bit Encryption Offered Abroad*, INFOWORLD, October 20, 1997, at 86.

[421] *See supra* note 309 and accompanying text.

[422] In fact, industry pressure appears to have already scored a victory at the White House. *See* Courtney Macavinta, *White House eases crypto limits* (visited Sept. 18, 1998) <http://www.news.com/News/Item/0,4,26427,00.html>. Following months of public and private debate, the White House relaxed its encryption policy by allowing non-licensed export of strong encryption products for use in international company intranets. *See id.* Free expression advocates fear, however, that the White House strategy of appeasing industry advocates "could divide the industry from the broader

B. How the World Has Responded So Far

As witnessed by the criticisms discussed above, encryption impacts cannot be resolved on a national scale. Due to the global nature of the world economy and the maturing Information Superhighway, national solutions also beget advantages or disadvantages for foreign people and firms. Unfortunately, global solutions have so far proved to be inadequate and no model has emerged which is embraced by all countries. This section discusses attempts at global agreement and provides a detailed summary of how countries have handled issues such as key recovery, and export and domestic regulations.

1. Initial International Cooperation

Initial attempts at a global solution involved the Coordinating Committee for Multilateral Export Controls (COCOM), which was an international organization devoted to synchronizing member country export restrictions on "strategic products and technical data."[423] In 1991 COCOM decided to allow export of mass-market and public domain cryptographic software, and most members followed its regulations, although the United States maintained separate regulations.[424] A year after COCOM dissolved in 1994, a follow-up organization was formed under the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*.[425] That agreement controlled

---

privacy groups in the debate going on in Congress." *Id.* (noting further that "concessions . . . to the commercial sector [do] nothing to enhance . . . access to strong encryption for individuals.").

[423] Bert-Jaap Koops, *Crypto Law Survey*, June 1998 (last modified June 11, 1998) <http://cwis.kub.nl/~frw/people/koops/cls2.htm> [hereinafter Koops *Survey*]. The 17 members included Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, The Netherlands, Norway, Portugal, Spain, Turkey, the United Kingdom, and the United States. *See id.* Further cooperating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland, and Taiwan. *See id.* The committee's main goal was to "prevent cryptography from being exported to 'dangerous' countries . . . such as Libya, Iraq, Iran and North Korea." *Id.*

[424] *See id.*

[425] *See id.* That agreement included 33 international signees: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian

the export of weapons and of dual-use goods[426] such as cryptography, and its provisions were quite similar to COCOM's provisions.[427] The *Wassenaar* Agreement initially excepted public-domain software, but encryption was later excluded from that exception.[428] Moreover, the regulations do not appear to cover export via the Internet.[429]

A more recent international encryption effort involved the Organization for Economic Co-operation and Development (OECD) and its *Recommendation of the Council Concerning Guidelines for Cryptography Policy.*[430] The guidelines are not binding on member states, but they do provide recommendations for member governments to consider as they decide national policies.[431] The guidelines describe the many issues involved with encryption and the benefits of market-driven development of cryptographic methods.[432] Key escrow, a contentious issue among OECD members, was neither endorsed nor prohibited in the report.[433] In fact, the guidelines allow broad interpretation for countries to choose privacy-centered or law enforcement-centered policies as they desire.[434] This broad reading was necessary given a rigid split between key escrow[435] advocates such as the United States, the United Kingdom, and France, and key escrow

---

Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. *See id.*

426 A dual-use good is one "that can be used both for a military and for a civil purpose." *Id.*

427 *See id.*

428 *See id.*

429 *See id.*

430 *See Recommendation of the Council Concerning Guidelines for Crytopraphic Policy* (visited Oct. 22, 1998) <http://www.oecd.org/dsti/sti/it/secur/prod/crypto1.htm> (describing the OECD guidelines released March 27, 1997).

431 *See* Koops *Survey, supra* note 423.

432 *See Guidelines for Cryptography Policy* (visited Oct. 22, 1998) <http://www.oced.org/dsti/sti/it/secur/prod/crypto2.htm>.

433 *See id.*

434 *See id.*

435 The "key escrow" term was not generally accepted by the members. Some countries preferred the term "trusted third party" (TTP) to "key escrow." *See* Stewart A. Baker, *Summary Report on the OECD Ad Hoc Meeting of Experts on Cryptography* <http://steptoe.com/276908.htm> (on file with author).

opponents such as Japan, Australia, and the Scandinavian countries.[436] Even countries supporting key escrow did not support the U.S. proposal that suggested all escrow agents be located in the United States.[437] Countries opposing key escrow prefer relying on warrants requiring defendants to decrypt their data.[438] Denmark's solution was to "shift the burden of proof to the defendant if he does not provide certain kinds of evidence that is within his control."[439] Although OECD discussions and guidelines provide insight into the two camps of international opinion, they do not provide a clear standard for all members to follow.

2. *A Global Shift Away from the Regulation and Key Escrow*

Although COCOM and OECD solutions encouraged the international community to define the issues in the encryption dispute, those solutions did not resolve core policy differences between the members. For example, few nations have identical regulations regarding encryption key escrow, export use, and domestic use. The following table presents a multi-government checklist of these issues as a distillation of surveys performed by Bert-Jaap Koops and the Global Internet Liberty Campaign:[440]

---

[436] *See id.*

[437] *See id.* (noting that Canada was concerned with U.S. control and that "[t]he UK, which was among the more supportive governments toward U.S. policy, nonetheless expressed the view that using U.S. export control laws to require that keys be escrowed in the U.S. would be a problem for the UK government").

[438] Australia supported this approach but had not solved the self-incrimination aspects of such a policy. *See id.*

[439] *Id.*

[440] *See* Koops *Survey*, *supra* note 423 (discussing developments restricting and favoring cryptography in each country); Global Internet Library Campaign, *Cryptography and Liberty: An International Survey of Encryption Policy* (visited Sept. 11, 1998) <http://www.gilc.org/crypto/crypto-results.html> [hereinafter GILC *Survey*] (analyzing encryption activities of each country and declaring a green, yellow, or red light for their position).

Region	Supports Escrow?	Export Regulations?	Domestic Regulations?
Anguilla	No[441]	No	No
Argentina	No[442]	No	No
Armenia	No	No[443]	No
Australia	No	License	No
Austria	No	License	Corporate use
Bangladesh	[444]		No
Belgium	No	License	No
Belize		No	No
Brazil	No	No	No
Bulgaria		Yes	Yes
Byelorussia			License
Campione d'Italia		License[445]	No
Canada	Yes	License[446]	No
China		Yes	Yes
Croatia		No	No
Czech Republic	No	No	No

[441] Not only does Anguilla not support U.S. initiatives such as key escrow, but it has also launched a civil disobedience campaign which allows one to send an encryption program to Anguilla in opposition to U.S. regulations. *See* GILC *Survey*, *supra* note 440.

[442] Although the survey found no regulation, restrictions are expected within the next year. *See* Koops *Survey*, *supra* note 423.

[443] Although Armenia currently has no policy against the use of encryption, the government recently established a Department of Information and Publications, which is planning to initiate cryptography legislation. *See* GILC *Survey*, *supra* note 440.

[444] Blank entries indicate that either the government has made no statement regarding the issue or the current legal state is unclear.

[445] This small Italian enclave, which is surrounded by Switzerland, generally adheres to Swiss laws. There is little or no restriction for encryption products in Switzerland. *See* GILC *Survey*, *supra* note 440.

[446] All types of cryptography can be transported between Canada and the United States. *See* Koops *Survey*, *supra* note 423.

Denmark	No	License	No
Estonia		License	
Falkland Islands		No	No
Finland	No	License	No
France	Yes	License[447]	Yes
Germany	Yes	License	No
Greece			No
Hong Kong		License[448]	
Hungary		License	No
Iceland			No
India		License	
Indonesia			Yes
Ireland	No	No	No
Israel		Yes	License[449]
Italy	Yes	License	Yes[450]
Japan	No	License[451]	No
Kazakhstan		License	License
Latvia	No	License	No
Lithuania		No	No
Malaysia		No	No
Mexico		No	
Mount Athos	No[452]	No	No
Nauru	No	No	No

[447] Authentication or integrity-only cryptography may be exported if a declaration dossier is deposited. *See id.*

[448] Licenses are required except for access-control equipment and authentication cryptography that cannot be used for encrypting files or text. *See id.*

[449] Licenses are virtually always granted. *See id.*

[450] A law demands accessibility of encrypted records for the treasury. *See id.*

[451] Export approvals are required for cryptography orders larger than 50,000 yen. *See id.*

[452] This religious, self-governed part of the Greek state warned Athens that any attempt to restrict encryption would be opposed by all its resident monks "as conscientious objectors." GILC *Survey*, *supra* note 440.

The Netherlands	Yes	License[453]	No
New Zealand	No	License	No
Norway		License	No
Pakistan			Yes
Philippines		No	No
Poland		License	No
Portugal			No
Romania		Yes	
Russia		Yes	License
Saudi Arabia		No	Yes[454]
Singapore		No	No[455]
South Africa		No	Yes
South Korea		Yes	No
Spain		Yes	No
Swaziland		No	No
Sweden	No	License	No
Switzerland		License[456]	Yes
Taiwan	Yes	Yes	No
Turkey		License	No
U.K.	Yes[457]	License[458]	No
U.S.	Yes	License	No[459]

[453] Licenses are required only for items capable of file encryption. *See* Koops *Survey*, *supra* note 423.

[454] It is reported that Saudi Arabian regulations prohibiting encryption use are widely ignored. *See id.*

[455] However, subscriber agreements with SingTel require approval from the Telecommunications Authority of Singapore. *See id.*

[456] Licenses are required for export to non-OECD countries. *See id.*

[457] Only confidentiality keys must be handed over, not signature keys. No distinction is made for dual-use keys. *See id.*

[458] Exports by intangible means, such as over the Internet, are not covered by the regulations. *See id.*

In addition to recognizing the variety of regulations being used by countries today, the recent battle over key escrow that is brewing between the United States and European nations is worth noting.[460] In particular, the success of the Labour party in the United Kingdom brought a new perspective to the U.K.'s regulatory policy. The United Kingdom, who had previously voiced strong support for key escrow, recently expressed a position that they "do not accept the 'clipper chip' argument developed in the United States for the authorities to be able to swoop down on any encrypted message at will and unscramble it."[461] Instead, they support the Danish approach of enabling "decryption to be demanded under judicial warrant (in the same way that a warrant is required in order to search someone's home)."[462] Finally, in outlining this new philosophy for the United Kingdom, the Labour party states that "[a]ttempts to control the use of encryption technology are wrong in principle, unworkable in practice, and damaging to the long-term economic value of the information networks."[463]

In addition to the Labour party opposition, U.S. policymakers

---

[459] Although export has been the regulatory focus up until now, Congressional and F.B.I. rumblings are moving the fight into the domestic arena. In particular, proposals from the House Intelligence Committee would "ban encryption inside the United States unless it contains features to provide law enforcement 'immediate access' to the plain text of encrypted information." Center for Democracy and Technology, *H.R. 695—The "Safe" Bill: Latest News* (last modified Apr. 22, 1998) <http://www.cdt.org/crypto/legis_105/SAFE/latest.html> [hereinafter CDT *Summary*]. These proposals come as amendments to a pro-encryption bill being debated in House committees. *See infra* notes 469-83 and accompanying text.

[460] Note that Japan already disagreed with the U.S. escrow policy. *See* Stewart A. Baker, *Decoding OECD Guidelines for Cryptography Policy*, 31 INT'L LAW. 729, 734-49 (1997). If the Europeans remain opposed to U.S. regulation proposals, key allies to the United States become China and the Russian republics—two regions which were historically viewed as oppressive to their citizens. *See id.*

[461] THE LABOUR PARTY, *The Labour Party—Information Superhighway* (visited Jan. 31, 1998) <http://www.labour.org.uk/views/info-highway/content.html> (outlining the British Labour Party's position on a variety of Internet issues including encryption).

[462] *Id.* This is consistent with their claim that it is unnecessary to "criminalise a large section of the network-using public to control the activities of a very small minority of law-breakers." *Id.*

[463] *Id.*

have received pressure from the European Commission (EC). In a report drafted by the European Internet Forum, the EC warned that "[r]estricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks .... It would not, however, totally prevent criminals from using these technologies."[464] This sentiment was echoed in January 1998 when Europeans criticized the United States "for its largely go-it-alone approach."[465] They emphasized that "the European Union's approach is for less regulation, more industry self-regulation, and more trust in market forces."[466] Deborah Hurley, a Harvard professor following encryption issues, remarked that "U.S. government representatives say that the rest of the world is going to do key escrow ... in the next five minutes."[467] Nevertheless, she noted that "only the United States and France are now pursuing such systems."[468] The next year appears to be pivotal for the United States to decide if it will continue its key escrow plans despite waning support. Such a proposition appears unlikely because U.S. software producers forced to include back doors for the U.S. government will be crippled by commercial forces since foreign governments are allowing their companies to provide more secure products.

VI. Conclusion

A. Current Legislative Options

The House and Senate of the 105th Congress have each introduced their own bills to "solve" the problems of current encryption export regulations. Representative Robert Goodlatte's original *Security and Freedom Through Encryption* (SAFE) *Act*[469]

---

[464] Dan Goodin, *EC report counterpoint to Clinton crypto*, (visited Sept. 11, 1998) <http://www.news.com/News/Item/0,4,15038,00.html>.

[465] Tim Clark, *Europeans slam U.S. crypto policy*, (visited Sept. 11, 1998) <http://www.news.com/News/Item/0,4,18079,00.html>.

[466] *Id.*

[467] *Id.* (suggesting that the United States and other key escrow advocates are "shoveling sand against the tide").

[468] *Id.*

[469] H.R. 695, 105th Cong. (1997).

loosens the export restrictions and offers key recovery as a voluntary option for companies but does not mandate it.[470] The bill claims that "the way to help law enforcement in this field is to encourage people to use strong encryption."[471] Nevertheless, since the bill was first introduced, it has been amended in five different committees, and the final bill presented to the House floor could look entirely different.[472] Senator John McCain sponsored one Senate counterpart in the form of the *Secure Public Networks Act*,[473] which has not yet reached the Senate floor. His approach gives government a more central role and encourages the use of accepted encryption solutions. The bill would require the use of key recovery systems when dealing with the government, and it also makes the use of encryption in criminal activity a separately punishable offense.[474] This approach has already received complaints that key recovery centers would only be used by law-abiding citizens while criminals would use overseas encryption solutions.[475] Another Senate solution, the *Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace* (E-PRIVACY) *Act*,[476] sponsored by Senator John Ashcroft,[477] chair of the Senate Judiciary's Constitution, Federalism, and Property Rights Subcommittee, is an attempt at compromise between the Goodlatte and McCain bills.[478] At first glance, it appears to follow

---

[470] *See* Corcoran, *supra* note 387 (summarizing the two competing encryption bills heading into the 105th Congress).

[471] *Id.* Representative Goodlatte stated that "[i]f an ounce of prevention is worth a pound of cure, then an ounce of encryption is worth a pound of subpoenas." *Id.*

[472] Some amendments added mandatory key escrow, and House Rules Committee Chairman Gerald Solomon has stated that he will not bring SAFE up for consideration unless it contains such a provision. *See* CDT *Summary*, *supra* note 459.

[473] S. 909, 105th Congress (1998).

[474] *See* Corcoran, *supra* note 387 (noting industry's frustration with the bill, because key recovery systems are impractical).

[475] *See id.*

[476] S. 2067, 105th Cong. (1998).

[477] John Ashcroft is chair of the Senate Judiciary Committee's Constitution, Federalism, and Property Rights Subcommittee.

[478] *See id.* Shortly after introducing this bill, Senator Ashcroft held hearings before the Senate Judiciary's Constitution, Federalism, and Property Rights Subcommittee which he chairs. *See Privacy in a Digital Age: Encryption and Mandatory Access, 1998: Hearings Before the Subcomm. on the Constitution, Federalism, and Property of*

Goodlatte's approach by emphasizing the need for only voluntary and market driven controls on the use and sale of encryption.[479] Unlike Senator McCain, Senator Ashcroft does not use government contracts as bait for producers to include key recovery.[480] Nevertheless, like Senator McCain's bill, the E-PRIVACY Act does grant exclusive licensing authority to the Secretary of Commerce with a process requiring pre-export technical review.[481] The E-PRIVACY Act has not reached the Senate floor but has garnered ten co-sponsors.[482] Progress has been slow on all of the bills before the 105th Congress, as Presidential impeachment issues have taken priority.[483]

B. Making an Informed Decision

This Comment has focused on the number of issues that make encryption export a contentious subject. There are no easy answers for balancing freedom of expression, rights to privacy, commercial interests, national safety, and international diplomacy. A key step to finding the answers is recognition of the important decisions that have been made along the way. In particular, a federal court has stated clearly that software is an expression protected by the First Amendment. Like the motion one detects in one's peripheral vision, the importance of this holding must not get lost in the focus on encryption. Both the House and Senate should begin hearings to understand the ramifications of protecting software as speech. As more communication in our society flows through computers, it is very possible that *Bernstein's* result will define expression into the twenty-first century.

---

the Senate Judiciary Comm., 105th Cong. (1998).

[479] *See* S. 2067 § 101(c)(1).

[480] *Cf.* S. 909 § 207.

[481] *See* S. 2067 § 302. The E-PRIVACY Act would minimize technical review for "generally available" technology without eliminating it. *See id.* Instead of product-by-product licensing review, the Act requires a one-time 15-day technical review after which export is allowed even without a license. *See id.*

[482] *See* S. 2067.

[483] *See* Corey Grice, *Tech issues in Lewinsky balance* (visited Sept. 18, 1998) <http://www.news.com/News/Item/0,4,26425,00.html> (noting that the Presidential scandal not only affects the economy, but also "detract[s] from the work at hand on Washington's high-tech docket.").

Next, given the need for international consistency in encryption regulations, both the House and the Senate should closely examine how other countries approach encryption regulation. Any law made here that limits encryption may only sacrifice U.S. citizens' security and its information economy's future. Thus, of the current House and Senate bills, only the original SAFE Act should be pursued while such foreign investigations take place. As its provisions are more lenient than the global consensus, passage of that bill would jeopardize neither privacy nor companies.

Finally, Congress and the White House should consider the constitutional reasoning set forth above, specifically that of the *Bernstein* series of decisions, and strike existing encryption export regulations. They have been labeled an unconstitutional prior restraint both by the courts and by the State Department. The federal courts supplied a remedy only to Bernstein[484] but *all* encryption providers should benefit from the same constitutional protections. Concerns for national security do not meet the threshold necessary for the *Freedman* factors,[485] and policy debates have suggested that security may be better served by wide-spread strong encryption.

The steps listed above may seem to suggest that the progress made by House and Senate committees should be jettisoned. To the contrary, the United States must learn from congressional, judicial, and international debates and stop pursuing a government stance for its own sake. If this can succeed, it will promote President Clinton's concern for "national security" while preserving the foundational belief in Justice Brandeis's beloved "free speech."

DANIEL R. RUA

---

[484] *See supra* notes 143-202 and accompanying text.

[485] *See supra* notes 319-24 and accompanying text.