SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Journal of International Law

Volume 30 | Issue 1

1998

Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective

J. Terrence Stender

TOO MANY SECRETS: CHALLENGES TO THE CONTROL OF STRONG CRYPTO AND THE NATIONAL SECURITY PERSPECTIVE

J. Terrence Stender[*]

[*] B.A., University of Washington, 1994; J.D. Candidate, 1998, Case Western Reserve University School of Law; former United States Navy, Naval Security Group cryptologist and signals intelligence situation analyst.

> Secrecy is a form of power. The ability to protect a secret, to preserve one's privacy, is a form of power. The ability to penetrate secrets, to learn them, to use them, is also a form of power. Secrecy empowers, secrecy protects, secrecy hurts. The ability to learn a person's secrets without her knowledge–to pierce a person's privacy in secret–is a greater power still.[1]
>
> — A. Michael Froomkin

> Now the reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge.[2]
>
> — Sun Tzu

I. INTRODUCTION

EVERYONE HAS SOMETHING TO HIDE. Some have more than others; some for more sinister reasons than others. Thus, the impetus for cryptography, the ancient craft of "secret writing," becomes all the more clear. For centuries, cryptography has served as the consummate shroud. Except now, it has gone high-tech. Once obscure and largely relegated to a select sphere consisting of "spooks,"[3] soldiers, statesmen, and a few mathematicians, cryptography has emerged from its cloak of secrecy, as a matter of discussion and as a matter of use. This age-old craft, tracing its roots to ancient Egypt, is now readily combined with modern computer technology to become more powerful than ever before, arguably more dangerous than ever before. As a result, encryption technology is regarded as a critical issue in the discussion over control and protection of information in this "information age."[4] As a new millenium dawns, technology, in this case

---

[1] A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and The Constitution*, 143 U. PA. L. REV. 709, 712 (1995) [hereinafter *Metaphor*].

[2] SUN TZU, THE ART OF WAR 144 (Samuel B. Griffith trans., Oxford University Press, 1963).

[3] A "spook" is a person involved in intelligence activity, typically intelligence collection. The word "spook" is also commonly used as an adjective to describe, "equipment, operations, or agencies involved in intelligence activity." NORMAN POLMAR & THOMAS B. ALLEN, SPY BOOK 528 (1997).

[4] *See* NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 19 (Kenneth W. Dam & Herb S. Lin eds., National Academy Press, 1996) [hereinafter CRISIS] ("The information age is enabled by computing and communications technologies (collectively known as information technologies) whose rapid evolution is almost taken for granted today. Computing and communications systems appear in virtually every sector of the economy and increasingly in homes and other locations"). The National Research Council is a part of the National Academy of Sciences. *Id.* at VI. Supremacy in "information" will likely serve as a determinant of

millenium dawns, technology, in this case encryption technology, has again revealed itself to be both friend and foe.[5]

Historically, those most genuinely interested in cryptography have been the governments of the world, or, more properly, their respective intelligence communities and militaries.[6] Typically, emphasis has been on the protection of state or military secrets and, of course, the collection and exploitation of adversaries' secrets.[7] However, with the rapid advances in computer technology over the last fifty years and the new vulnerability that technology has brought with it, encryption technology has become a valued tool for both businesses and individuals in the protection of proprietary and personal information.[8]

---

political, or even economic reasons is merely the collection of information. *See* LOCK K. JOHNSON, SECRET AGENCIES 2 (1996) (stating that "intelligence is information, a tangible product collected and interpreted in order to achieve a sharper image of political and military conditions worldwide").

[5] To be sure, technology has always been a source of both good and evil, progress and regression. However, recent advancements in computer technology have made encryption technology an even greater friend, an even greater foe. Encryption is now easier to use, cheaper to acquire, and generally more accessible to a broad spectrum of people and organizations, who, quite naturally, and quite historically, are capable of both good and evil. *See* Dorothy E. Denning & William E. Baugh, Jr., *Key Escrow Encryption Policies and Technologies*, 41 VILL. L. REV. 289, 289 (1996) [hereinafter *Key Escrow*] ("In today's information age, encryption is considered essential to ensure the security of electronic data and transactions. At the same time, however, there is growing recognition that the spread of powerful encryption technology is not entirely beneficial").

[6] *See* CRISIS, *supra* note 4, at 53. *See also* HARRY HOWE RANSOM, CENTRAL INTELLIEGENCE AND NATIONAL SECURITY 116 (1959) ("Problems as old as intelligence itself are the secure communicating of secret information and the interception of such information transmitted by foreign governments or their espionage agents. The use of professional code makers and code breakers is perhaps as old as diplomacy and espionage").

[7] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, Preface, XIX (2d ed., 1996) (noting that "[f]or many years . . . cryptography was the exclusive domain of the military. The National Security Agency and its counterparts in the former Soviet Union, England, France, Israel, and elsewhere, have spent billions of dollars in the very serious game of securing their own communications while trying to break everyone else's . . . . While classical cryptography has been long used by ordinary citizens, computer cryptography was the exclusive domain of the world's militaries since World War II. Today, state-of-the-art computer cryptography is practiced outside the secured walls of the military agencies").

[8] *See* Sean M. Flynn, *A Puzzle Even The Codebreakers Have Trouble Solving: A Clash of Interests Over The Electronic Encryption Standard*, 27 LAW & POL'Y INT'L BUS. 217, 218 (1995). Banking, for example, uses encryption to protect ATM (automat-

In the United States a battle has emerged — code makers versus code breakers.[9] On one hand is the government, code breakers, charged with the heavy burden of protecting public safety.[10] On the other hand, there are the code makers, which include a potpourri of interests — for example, corporations or companies interested in protecting proprietary information or confidential records, computer industry executives drawn to the exploitation of a potentially very profitable technology, and those concerned with protecting individual privacy and freedom of speech.[11]

All of these interests, whether it be government, business or individual, however, are not necessarily at odds; although, this is often difficult to perceive given the level of invective surrounding the debate. Secure communications, secure data storage, individual privacy and a robust economy are with little doubt within the most basic national interest.

BUS. 217, 218 (1995). Banking, for example, uses encryption to protect ATM (automated teller machines) passwords and electronic funds transfers. The move away from largely cash-dominated transactions to a "digital cash" world portends even greater use of encryption in banking. Businesses wanting to protect commercial and trade secrets are increasingly making use of encryption. *See Metaphor, supra* note 1, at 719-34 (sketching current uses and future needs of encryption to secure communications and maintaining data security).

[9] *See* Dorothy E. Denning, *Encryption Policy and Market Trends,* (visited Mar. 12, 1998) <http://guru.cosc.georgetown.edu/~denning/crypto/Trends.html#1> [hereinafter *Encryption Policy*] (arguing that the "driving forces behind encryption policy and technology are served by two opposing functions: code making and code breaking"). Denning uses the term "code making" to refer to the use and development of encryption products. Whereas, code breaking means "acquiring access to the plaintext of encrypted data by some means other than the normal decryption process used by the intended recipient(s) of the data." *Id.*

[10] There is little doubt that the U.S. government is both a substantial maker and *breaker* of cryptography. The United States National Security Agency is charged with a dual duty — making U.S. code unbreakable, while at the same time breaking opposing code with impunity. *See Online Encryption Technology: Hearing on S. 377, A Bill to Loosen the Export Restrictions on Encryption Technology Before the Senate Committee on Commerce, Science, and Transportation,* 105th Cong. (Mar. 19, 1997) [hereinafter *Online Encryption Technology: A Bill to Loosen Restrictions*] (written statement by William P. Crowell, Deputy Director, National Security Agency). However, in the debate over control of cryptography, the government's primary interest has been in maintaining their already preeminent capability in *breaking* cryptographic code — that is, protect national security by exploiting signals intelligence gleaned from adversaries' cryptography. *See* CRISIS, *supra* note 4, at 46-48, 128.

[11] These categories are clearly not fully representative of the numerous interests and stakeholders involved in the debate over cryptographic controls, but the dichotomy does serve to put the two primary sides into a broad but informative perspective. Additionally, it is important to remember that many of these interests invariably overlap.

However, "[t]he greatest dilemma arises from the fact that techniques that protect against illicit eavesdropping and data theft also threaten to prevent licit access to communications and data by law enforcement and intelligence agencies."[12] This dilemma strikes at the core of the debate about national security controls on encryption technology.

A central concern of this Note is to present and briefly critique significant challenges to the U.S. export control regime governing encryption technology. However, principally, the survey of recent challenges to the control of encryption will ultimately serve as the necessary preface to consideration of the question of national security, as it relates to encryption technology. Specifically, this Note examines legislative efforts to liberalize export licensing controls and constitutional court challenges to limit or eliminate their effect. This Note makes no attempt, though, to explicitly argue for or against decontrol of encryption; rather, this Note presents the relevant legal and legislative challenges to continued control of encryption technology as a backdrop to the presentation of the national security perspective. The national security perspective, long misunderstood and consistently misrepresented, suggests that further proliferation[13] of encryption, principally, *strong* encryption,[14] presents a credible and

---

[12] *See* A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15, 16 [hereinafter *Planet Clipper*]. As Froomkin also aptly points out, this "policy dilemma is especially acute in the United States because widespread encryption imposes a particularly severe cost on U.S. intelligence-gathering capabilities . . . . U.S. [signals]-intelligence capabilities are presumed to be the best in the world; if so, the U.S. has the most to lose from a move towards a world in which communications traffic is routinely protected with encryption so strong that it cannot be decrypted easily, and perhaps not at all. Widespread high-quality encryption not only lessens the U.S. government's ability to eavesdrop on foreign communications, but threatens to make it difficult, perhaps impossible, to conduct traffic analysis." *Id.*

[13] Any reference to "proliferation" herein is a distinct reference to further proliferation outside the borders of the United States. Arguably, attempts to control the export of cryptographic products also limit to one degree or another domestic proliferation.

[14] "Strong cryptography refers to cryptographic systems that are very difficult to break." CRISIS, *supra* note 4, at 382. Strong cryptography is considered encryption with a key length longer than 40-bits and the term will be used as such herein. *See* CRISIS, *supra* note 4, at 121. While the U.S. government controls, to one extent or another, all export of encryption technology, regardless of strength, their primary concern and arguably their focus is control of strong encryption. *Id.* at 117-18 (noting that the weaker encryption enjoys more liberal export than strong encryption). *See also infra* note 57 for further discussion of strong encryption. This Note's focus is similarly on *strong* encryption. However, strong encryption is an inherently relative and fluid concept. *See* SCHNEIER, *supra* note 7, at 8. "Cryptography is more concerned with

recognizable threat to U.S. national interests, and export restrictions, at present, provide the most effective means to blunt that threat and therefore are necessary. While, arguably, the national security perspective is not, per se, a legal argument for or against decontrol, it stands to form the bedrock foundation for upholding controls on encryption, whether the context is a policy or a legal.[15] Consequently, its presentation is a necessary predicate to any assessment of the validity or invalidity of the U.S. control regime on encryption technology.

Part II of this Note provides a background of the relevant history, terms, and mechanics of cryptography. Part III reviews prior and current U.S. policy and law regarding cryptography. Part IV examines recent challenges to the government's crypto[16] control regime. Specifically, Part IV looks at pending legislation before Congress to further liberalize export controls governing encryption technology. Additionally, several court cases challenging the constitutionality of the controls are reviewed. Part V presents the national security perspective, principally delineating the specific threats that further proliferation poses to U.S. national security. Finally, the inevitable conclusion is that further proliferation of strong encryption presents a significant risk to national security, and, consequently, efforts to completely decontrol crypto are at best, unwise, at worst, rash and foolhardy. However, this conclusion understands that efforts to

---

cryptosystems that are computationally infeasible to break. An algorithm is considered computationally secure (sometimes called *strong*) if it cannot be broken with available resources, either current or future." *Id.*

[15] *Compare Encryption Export: Hearing on Encryption and H.R. 695 Before the House Subcommittee on International Economic Policy and Trade and the House International Relations Committee* (May 8), 105th Cong. (1997) (statement of Robert S. Litt, Deputy Assistant Attorney General) (testifying that while the Clinton Administration supports the proliferation of robust encryption for the protection of privacy and promotion of commerce, the government must remain mindful of its "other principal responsibilities: to protect public safety and national security against the threats posed by terrorists, organized crime, foreign intelligence agents, and others . . . . [W]e are gravely concerned that the proliferation and use of unbreakable encryption would seriously undermine out ability to protect the American people"), *with* Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1438 (N.D. Ca. 1996) (finding that governmental licensing schemes on encryption technology carry a heavy presumption against validity when they act as a prior restraint on speech and noting that efforts at prior restraint have been struck down in the face of national security concerns when those concerns were too vague or lacking in direct, immediate, and irreparable damage). *See* New York Times Co. v. United States, 403 U.S. 713 (1971) (finding that the government failed to meet its burden to impose a restraint on the publication of classified military papers regarding the conflict in Vietnam).

[16] The term "crypto" is commonly used in place of "cryptography" or "encryption" and will be used at times herein as well.

loosen or revise the impact of certain controls, which impact upon both the computer industry and private citizens, present a significant interest that cannot be wholly discounted. As a result, a compromise, principally found in the form of an escrowed-encryption scheme, appears to be a viable alternative to either extreme — that is, unmitigated decontrol of strong encryption versus an absolute proscription of the export of strong encryption.[17]

II. CRYPTO 101[18]

> There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading you files.[19]
>
> — Bruce Schneier

> [I]f I take a letter, lock it in a safe, hide the safe somewhere in New York, then tell you to read the letter, that's not security. That's obscurity. On the other hand, if I take a letter and lock it in a safe, and then give you the safe along with the design specifications of the safe and a hundred identical safes with their combinations so that you and the world's best safecrackers can study the locking mechanism — and you still can't open the safe and read the letter — that's security.[20]
>
> — Bruce Schneier

A. What Is Cryptography?

Cryptography is the art and science of keeping information secret by

---

[17] Escrowed encryption involves numerous questions far beyond the scope of this Note. However, when speaking about escrowed encryption as an alternative here, it is important to note that the focus is entirely outward—that is, the export of encryption, in an escrowed form. Although there is much debate whether mandatory escrow of encryption for export in effect affects domestic encryption availability, that issue is not considered here. Thus, for purposes of this Note, the author assumes controls on exported encryption primarily will affect foreign users and that is, in fact, their primary purpose.

[18] This section serves as a short primer on crypto terms and concepts as well as setting the stage for a fuller discussion of export control of encryption technology. Cryptography is a highly complex art and science. With rapid advances in computer technology, it has become even more complex and technical. This background section is intended to provide only the most basic understanding of cryptography. *See* Charles Merrill, *A Cryptography Primer*, 443 PLI/PAT 187 (1996), *available in* WESTLAW, for an excellent overview of basic cryptography, specifically geared toward the attorney.

[19] SCHNEIER, *supra* note 7, at Preface, XIX.

[20] *Id.*

using a code[21] or cipher.[22] Encryption is the process of transforming original information into an unreadable or unintelligible form — gibberish.[23] The original, unencrypted, information is referred to as plaintext.[24] The transformed, encrypted, information is called ciphertext.[25] Ciphertext is returned to its original form, plaintext, by the process of decryption.[26] A mathematical function, essentially just a set of rules or series of mathematical steps, is used for the process of encryption and decryption. This is a cryptologic algorithm, sometimes referred to as a cipher.[27] Most modern cryptographic systems utilize a "key" in conjunction with the algorithm.[28] A cryptosystem consists of the algorithm, all possible

---

[21] Codes and ciphers, although the terms are often used interchangeably, are not the same. *See* DAVID KAHN, THE CODEBREAKERS xvi (2d. ed. 1996) [hereinafter CODEBREAKERS] (distinguishing cryptographic code from cipher). A code is a cryptosystem that deals with linguistic units, like words, phrases, and sentences. *See* SCHNEIER, *supra* note 7, at 1. A code is a system of concealing communication that relies on pre-arranged mapping of meanings, often found in a "code book." *See* CODEBREAKERS, at xvii. A good example of using a cryptographic code is Paul Revere's "one, if by land, and two, if by sea." *See Metaphor, supra* note 1, at 713 (*quoting* HENRY W. LONGFELLOW, *The Landlord's Tale: Paul Revere's Ride, in* 4 THE POETICAL WORKS OF HENRY WADSWORTH LONGFELLOW 25, 25 (1966)). The basic unit of a cipher, on the other hand, is the letter. *See* CODEBREAKERS, at xvi. Code-based cryptosystems have limited applicability in computer-devised encryption schemes. *See* SCHNEIER, *supra* note 7, at 31. As Bruce Schneier explains, "Codes are only useful for specialized circumstances. Ciphers are useful for any circumstance. If your code has no entry for *anteaters*, then you can't say it. You can say anything with a cipher." SCHNEIER, *supra* note 7, at 9. Modern encryption technology uses cryptographic algorithms — ciphers. *See id.* at 2.

[22] *See* SCHNEIER, *supra* note 7, at 1. The word "cryptography" originates from the Greek *krypte<kryptós*, "secret, hidden," and *graphia*, "writing." *See* FRED B. WRIXON, CODES AND CIPHERS 46 (1992). Since time immemorial, cryptography has been merely "the science of keeping information secret from those not authorized to see it." CRISIS, *supra* note 4, at 374. However, "[t]oday, cryptographic methods help solve critical information-age problems . . . ." *Id.* For example, cryptography now deals with complex problems of data confidentiality, data integrity, and subject authentication. *See id.*

[23] *See* Deborah Russell & G.T. Gangemi, Sr., *Encryption, in* COMPUTER SECURITY BASICS 165, at 165-79 (1991), *reprinted in* BUILDING IN BIG BROTHER 10, at 14 (Lance J. Hoffman ed., 1995).

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *See* SCHNEIER, *supra* note 7, at 2.

[28] *See* Russell & Gangemi, *supra* note 23, at 14. The cryptographic algorithm "mathematically applies the key, which is usually a long string of numbers, to the

plaintexts and ciphertexts, along with the keys.[29] "Cryptanalysis is the art and science of decrypting ciphertext without access to the key," essentially, "code breaking."[30]

B. How Does It Work?

A particular encryption is typically achieved by taking plaintext, which may be a stream of bits, a text file, a bitmap . . . or whatever, and converting it to ciphertext by use of a key and an algorithm.[31] Decryption then works in the reverse, running the ciphertext back through an algorithm-key combination resulting in the original plaintext.[32] Generally, the strength of a cryptographic system is gauged by the length of its key and the complexity of its algorithm.[33]

Modern cryptography is expressed by two general types of key-based algorithms — the symmetric, also called single key or secret key, and the asymmetric, also called public key.[34] In a secret-key system both the encryption key and the decryption key are the same.[35] That is, everyone that needs to decrypt the message must have the key distributed to them.[36] Secret-key cryptographic schemes, however, possess an inherent vulnerability — the problem of finding a trusted method to distribute the key, and moreover, protecting the key while in custody.[37] Consequently,

---

information being encrypted or decrypted." *Id.*

[29] *See* SCHNEIER, *supra* note 7, at 4.

[30] *Id.* at 5. "Successful cryptanalysis may recover the plaintext or the key." *Id.* Crypotology refers to the study of cryptography and cryptanalysis. *See id.* at 1. The Department of Defense defines cryptology as the science which involves hidden, disguised or encrypted communications, embracing both communications security and communications intelligence. *See* DEPARTMENT OF DEFENSE, THE JOINT CHIEFS OF STAFF, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 175 (1974).

[31] *See* SCHNEIER, *supra* note 7, at 2.

[32] *See id.*

[33] *See* CRISIS, *supra* note 4, at 353.

[34] *See* SCHNEIER, *supra* note 7, at 4.

[35] *See id.* at 4-5.

[36] *See id.*

[37] *See id.* How well a key remains protected is a fundamental element concerning the security of the encryption. *See id.* at 7 (describing how the best way to break a cryptosystem is bribe, or steal, or blackmail your way to getting across the key). *See* Ira S. Rubenstein, *Export Controls on Encryption Software, in* COPING WITH U.S. EXPORT CONTROLS 1994, at 177, 183 (PLI Com. L. & Prac. Series No. A-705, 1994) (noting that secret-key encryption requires a trusted method for distributing keys and while possible in a military setting, "it is impractical in modern communications systems, where there is no secure channel for exchanging key secrets among millions of potential users"); RSA Laboratories, *Answers to Frequently Asked Questions About*

symmetric, secret-key encryption was mostly impracticable for widespread commercial or personal use.[38]

The critical key-management problem facing secret-key cryptography was solved in the mid-1970s, when two Stanford University scientists, Whitfield Diffie and Martin Hellman,[39] invented public-key encryption.[40] In public-key encryption, the key used for encryption is different from the key used for decryption.[41] Moreover, although the keys are mathematically related, as would be necessary to complete the encryption/decryption process, and essentially form a matched pair, it is computationally infeasible to derive one key from the other. "Therefore, the system allows users to openly publish one key in a phone-book like directory (the 'public key'), while keeping the other key private (the 'private key')."[42] Public key encryption allows parties to exchange encrypted messages by using and revealing only their public keys, without ever having to exchange private keys.[43]

Cryptographic strength is dependent both upon the mathematical structure of the algorithm itself and the length of the key used.[44] Generally, the longer the key, the stronger the encryption.[45] This is particularly

---

Today's Cryptography, reprinted in BUILDING IN BIG BROTHER, 34 (Lance J. Hoffman ed., 1995) ("The main problem is getting the sender and receiver to agree on the secret key . . . . If they are in separate physical locations, they must trust a courier, or a phone systems, or some other transmission system to not disclose the secret key being communicated. Anyone who overhears or intercepts the key in transit can later read all messages encrypted using that key").

[38] *See also* Rubenstein, *supra* note 37, at 183.

[39] *See id.*

[40] *Id.*

[41] *See* SCHNEIER, *supra* note 7, at 4.

[42] Rubenstein, *supra* note 37, at 183. A hypothetical might be helpful: A wants to send B a confidential e-mail message. A looks up B's public key in a public-key directory, probably found at some Internet site. A encrypts her e-mail message using B's public key. A's encrypted message is then sent normally through the Internet. B receives the message, which is in an unreadable form. B then decrypts A's e-mail message using his own private key. Consequently, as long as B's private key remains private, only he can read A's messages. The problems related to single key trusted distribution are solved. *See id.* at 189.

[43] *See id.*

[44] *See* CRISIS, *supra* note 4, at 63.

[45] *See id.* (describing how increasing the key size from 40 bits to 56 bits would increase the time it takes to decipher the message (using a single computer) from 11.5 days to 2,000 years). For example, "[f]or well-designed symmetric cryptographic systems, 'brute-force' exhaustive search — trying all possible keys with a given decryption algorithm until the (meaningful) plaintext appears — is the best publicly known cryptanalytic method." *Id.*

the case when a "brute-force" attack is initiated to break the key.[46] However, "[a]lthough key length is significant to the strength of an algorithm, weaknesses in key management protocols or implementation can allow keys to be cracked that would be impossible to determine by brute-force."[47] The strength of a cryptographic algorithm is proportional to the length of the key used — typically expressed in bits.[48]

C. What Is Escrowed Encryption?

Escrowed encryption is at its most basic level merely a tool — a tool utilized to provide access to encrypted information, whether it be for intelligence or law enforcement purposes or merely because the encryption key was lost, forgotten or misplaced.[49] "Escrowed encryption is the basis for a number of administration proposals that seek to reconcile needs for information security against the needs of law enforcement and to a lesser extent national security."[50]

---

[46] *See id.* A "brute-force" attack can be undertaken with a powerful computer or set of computers that attempt every possible key combination until the actual key is found. *See id.* at 124. For example, in 1995 a French student cracked a forty-bit key in eight days using 120 workstations and several supercomputers. *See* Dorothy E. Denning & William E. Baugh, *Decoding Encryption Policy* (visited Oct. 11, 1996) [hereinafter *Decoding Encryption*] <http://www.SecurityManagement.com/library/000065.html (10/11/96)>.

[47] *See Encryption Policy*, *supra* note 9. For example, two Berkeley students found that the "keys generated for Netscape could be hacked in less than a minute because they were not sufficiently random." *Id.*

[48] *See Planet Clipper*, *supra* note 12, at 20.

[49] *See* CRISIS, *supra* note 4, at 168.

[50] *Id.* at 167. The "Clipper chip" was the government's initial attempt at presenting a viable key escrow policy to the public. It was met with tremendous opposition. *See* Richard L. Field, *Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U. L. REV. 967, 993 (1997) (describing in detail the various efforts by the Clinton administration to produce a viable key escrow system). The term "escrow" was introduced in the context of the 1993 Clipper initiative by the Clinton administration. At the outset "escrowed encryption" had a very specific meaning — a mechanism for assuring law enforcement access to encrypted voice communication from wiretaps. However, during the several years of ensuing debate over crypto, terms such as "escrow," "key escrow," or "escrowed encryption" have engendered a much broader meaning, and in some cases different meanings altogether. *See* CRISIS, *supra* note 4, at 168. "[Escrowed] is no longer the very precise restricted concept embodied in the Clipper initiative . . . . Escrow as a concept now applies not only to the initial purpose of assuring law enforcement access to encrypted material, but also to possible end-user or organizational requirements for a mechanism to protect against lost, corrupted, or unavailable keys." *Id.*

An escrowed encryption system is where either in part or in whole a crypto key is kept "in escrow" by a trusted third party.[51] The key could be released only to authorized parties, either predetermined or by court order.[52] In essence, an escrowed encryption system enables a third party to keep a copy of the encryption key needed to decrypt all communications using the escrowed standard.[53] "These activities share the premise that it is reasonable for the government to request, and in some cases require, that private persons communicate in a manner that makes interception by the government at least practical and preferably easy."[54] By virtue of holding or having access to a "back-door" key, the government is willing to let stronger crypto out into the mainstream, or in other words, allow the export of strong crypto.[55] Since the Clinton Administration's 1993 Clipper initiative, one of many different escrow schemes proposed, some form of an escrowed encryption scheme has

---

[51] *See* Dorothy E. Denning, *The U.S. Key Escrow Encryption Technology, in* COMPUTER COMM., July 1994, *reprinted in* BUILDING IN BIG BROTHER, 111 (Lance J. Hoffman ed., 1995) (describing the technical aspects of key escrow technology). "The term 'escrow,' as used conventionally, implies that some item of value (*e.g.*, a trust deed, money, real property, other physical object) is delivered to an independent trusted party that might be a person or an organization (i.e., an escrow agent) for safekeeping, and is accompanied by a set of rules provided by the parties involved in the transaction governing the actions of the escrow agent." CRISIS, *supra* note 4, at 167.

[52] *See* OFFICE OF THE ATTORNEY GEN., U.S. DEP'T OF JUSTICE, ATTORNEY GENERAL MAKES KEY ESCROW ANNOUNCEMENTS (1994), *reprinted in* BUILDING IN BIG BROTHER, 241 (Lance J. Hoffman ed., 1995) (outlining the basic methodology of key escrow). *See also* U.S. DEPARTMENT OF JUSTICE, AUTHORIZATION PROCEDURES FOR RELEASE OF ENCRYPTION KEY COMPONENTS IN CONJUNCTION WITH INTERCEPTS PURSUANT TO TITLE III AND FISA (1994), *reprinted in* BUILDING IN BIG BROTHER, 243 (Lance J. Hoffman ed., 1995) (outlining the procedure by which the department may release escrowed key components that use key-escrow encryption methods, as proposed Feb. 4, 1994).

[53] *See* CRISIS, *supra* note 4, at 167 ("The underlying notion is that the escrow agent is a secure haven for temporary ownership or possession of the item, is legally bound to comply with the set of rules for its disposition, functions as a disinterested extratransaction party, and bears legal liability for malfeasance or mistakes"). *See also Metaphor, supra* note 1, at 742-43.

[54] *See Metaphor, supra* note 1, at 743.

[55] *See Encryption Export: Hearings Before the Subcommittee on International Economic Policy and Trade*, 105th Cong. (1997) (testimony of William A. Reinsch, Under Secretary for Export Administration) [hereinafter *Encryption Export*]. *See generally Prepared Testimony of William A. Reinsch, Under Secretary for Export Administration on Encryption Policy Before the House Committee on International Relations, Subcommittee on International Economic Policy and Trade*, 105th Cong. (1997) [hereinafter *Reinsch Testimony*].

served to form the basis for encryption control.[56] The government has generally seen escrowed encryption as a viable alternative to what would otherwise seem to be a zero-sum situation.[57] Escrow became a compromise between the needs of the U.S. national security establishment and the concerns of individuals and businesses.[58] However, opponents to any controls on encryption technology have generally regarded escrowed encryption proposals as yet another attempt to back-door, Big-Brother into purely "private" matters.[59]

D. Historical Perspective

Cryptography has a very long and very rich history.[60] The earliest traces of cryptography date back nearly 3,000 years to early Egyptian hieroglyphic symbol substitutions.[61] "From the Spartans to Julius Caesar, from the Old Testament ciphers to the Papal plotters of the Fourteenth Century, from Mary, Queen of Scots to Abraham Lincoln's Civil War ciphers, cryptography has been part of war, diplomacy, and politics."[62] For example, Gaius Julius Caesar is accredited with successfully using Greek letters to mask his Latin communiqués. Caesar also used rearrangements of plaintext alphabet, with only the intended recipient knowing how to shift the alphabet back to a readable form.[63] The American Revolution

---

[56] *See* CRISIS, *supra* note 4, at 215, 414-20.

[57] *See Encryption Export, supra* note 55. *See generally Reinsch Testimony, supra* note 55.

[58] *See Encryption Export, supra* note 55. The debate over export controls is closely linked to the debate over escrowed encryption, as proposals by the Clinton administration for relaxation of export controls are almost entirely predicated on adoption of some variant of an escrowed key regime. Opponents of crypto export controls argue that the national security argument is largely a red herring, and that the actual motive behind preservation of export controls on encryption is to provide leverage for imposing an unwanted escrowed encryption standard on the public. *See generally The Promotion of Commerce Online in the Digital Era Act of 1996, or Pro-CODE Act: Hearings on S. 1726 before the Comm. on Commerce, Science and Transp.*, 104th Cong. (1996) [hereinafter *Pro-CODE Hearings*].

[59] *See* ANDRE BACARD, THE COMPUTER PRIVACY HANDBOOK 100 (1995).

[60] *See generally* CODEBREAKERS, *supra* note 21 (comprehensively sketching the history of cryptography from ancient Egypt to India, Mesopotamia, Babylon, Greece, and further into Western civilization, and finally dawning at the technology-laden modern era). Kahn's book, originally published in 1967, but recently revised and updated, remains to this day the most definitive work on the history of cryptography.

[61] *See* CODEBREAKERS, *supra* note 21, at 71-73.

[62] Russell & Gangemi, *supra* note 23, at 11.

[63] This came to be know as the "Caesar Substitution." *See* WRIXON *supra* note 22, at 29, 34; *see also* Luke Seemann, *Keys to Secret Drawers*, (Sept. 29, 1996)

has a very rich history regarding organized cryptography and cryptanalysis.[64] During the American Revolution, Benedict Arnold, while arranging his betrayal of West Point to the British, passed clandestine correspondence to John Andre by employing a book code based on volume I of the fifth Oxford edition of Blackstone's famed legal classic, *Commentaries on the Laws of England*.[65]

However, colonial efforts and advancements in crypto paled in comparison to those made during World War II. Cryptography played a very substantial role in World War II. "The development of modern cryptography owes much to the research conducted under the pressures of World War II, and particularly to the breaking of the Engima[66] machine."[67] The cracking of the German "Ultra" codes and the Japanese "Purple" codes on the other side of the ocean contributed substantially to the allied victory in World War II.[68] "In the decades since World War II, the use of computers to break codes has transformed the code breaking game and has contributed greatly to the use of cryptography in military and intelligence applications, as well as in systems used in everyday computer systems."[69]

<www.stardot.com/~lukeseem/j202/essay.html> ("The earliest systems of encryption were the so-called 'Caesar Ciphers' used by early generals to send secret messages. They used the simplest of algorithms. Each letter was replaced by another letter a certain distance away in the alphabet. 'A' would become 'E' and 'B' would become 'F,' for example. Today, however, the science of cryptology is an advanced form of mathematics filled with esoteric jargon such as 'graph isomorphism,' 'multiplexers,' and 'one-way hash functions'").

[64] *See generally* CARL VAN DOREN, SECRET HISTORY OF THE AMERICAN REVOLUTION (1941) (discussing the use of code during numerous Revolutionary War intrigues). *See also* CODEBREAKERS, *supra* note 21, at 176-84.

[65] *See* CODEBREAKERS, *supra* note 21, at 176-77. Arnold and Andre's code used three numbers to make a word. To encode plaintext, they would search for necessary words for the message in a book, then, when a word was found, its page number, line number, and word number were written down. The first number represented the page, the second the line, and the third the word. "Words not in the book were to be spelled out, and these codenumbers distinguished from the others by drawing a line through the last number, which then represented the position of a letter in that line instead of a word." It was considered unbreakable but ultimately discarded as being impractical and highly cumbersome. *Id.* at 177.

[66] The Enigma was a cipher machine invented by Arthur Scherbius early in the 20th century and used by the German Navy and foreign office as early as 1926. *See* Russell & Gangemi, *supra* note 23, at 12; WRIXON, *supra* note 22, at 60.

[67] *See* Russell & Gangemi, *supra* note 23, at 12; DAVID KAHN, SEIZING THE ENIGMA (1991) (providing a full account of the breaking of the Enigma code and an interesting discussion of the Enigma machine).

[68] *See* CODEBREAKERS, *supra* note 21, at 67, 613.

[69] Russell & Gangemi, *supra* note 23, at 14.

III. CONTROLS ON PROLIFERATION OF STRONG CRYPTO[70]

> As far as the Department of Defense is concerned, cryptography and nuclear technology are two of the most sensitive areas in science and research since they both represent military strength.[71]
>
> — Winn Schwartau

> Cryptographic software is not barred from export from the United States, but is controlled through a licensing process.[72]
>
> — *Junger v. Christopher*

Generally, there is no control regime in place to control the proliferation of encryption technology purely within the United States.[73] However, even that issue is highly contested, as those supporting relaxation of current export controls on cryptography claim that controls on export implicitly restrict domestic use.[74] The government has often and loudly stated that it does not seek to control domestic use of cryptography. However, as with almost every other issue in this highly charged debate, opponents dismiss those assertions as merely Big Brother-esque lip ser-

---

[70] Encryption with a key length longer than 40-bits is generally considered to be strong encryption. *See supra* note 14 and accompanying text. Although the government in practice and substantially in effect controls *all* encryption, this Note is concerned with controls and challenges as they relate to further proliferation of *strong* encryption. This, no doubt, is a difficult distinction to make given the all-encompassing and overlapping nature of the crypto control policy, challenges thereto, and the subject matter itself; however, it is a necessary distinction to make if the national security perspective is to be fully appreciated. While proliferation of any encryption (i.e., weak or strong) *ipso facto* presents a threat (of some kind) to national security, on balance, the stronger the crypto, the stronger the threat. As a result, suggestions for further control of *strong* encryption do not necessarily lend themselves to support of control of *all* encryption, weak or strong. As noted *supra* the strength of the encryption, measured by key length, is generally representative of its ability to repel attack or lend itself to cryptanalysis. However, this is by no means the only factor that affects the fundamental "security" of encryption. *See Encryption Policy*, *supra* note 9 (noting that poor management or implementation can weaken otherwise secure encryption).

[71] WINN SCHWARTAU, INFORMATION WARFARE 148 (1994).

[72] Junger v. Christopher, No. 96 CV 1723, at ¶ 21 (N.D. Ohio Feb. 6, 1997) (defendant's proposed findings and facts and conclusion of law).

[73] *See Showdown on Encryption*, WASH. POST, May 25, 1997, at C6.

[74] *See id.* (noting that opponents of controls claim that it is too complicated to market full strength encryption for domestic use and a weaker encryption for foreign use).

vice.[75] But the fact remains that no explicit controls exist on cryptography domestically.[76]

A. Prior Control of Encryption Under ITAR

United States policy concerning control of strong encryption was significantly altered at the end of 1996. As a result, prior to outlining the current controls on the availability of strong encryption, there will be a brief review of the previous control regime. This review of prior policy will provide the necessary context for discussion of the current control regime.

Prior to December of 1996, the distribution of encryption products outside of the United States was governed by the Arms Export Control Act (AECA)[77] and the International Traffic in Arms Regulations (ITAR).[78] ITAR control items are listed on the U.S. Munitions List (USML) and administered by the Office of Defense Trade Controls, Department of State.[79] The Commerce Department administers the Export Administration Regulations (EAR). EAR regulate the export of "dual-use"[80] items, which are listed on the Commerce Control List (CCL).[81] Items listed on the CCL typically include data authentication and password protection encryption devices.[82] Generally, items "capable of

---

[75] *Id.*

[76] *Id.*

[77] *See* 22 U.S.C. 2778 (1994).

[78] *See* 22 C.F.R. § 120 (1997). The statutory authority for ITAR rests in the Arms Export Control Act, as amended at 22 U.S.C 2778 (1994).

[79] *See* 22 C.F.R. § 121.1 XII(b)(1) (1997) (specifically including on the U.S. Munitions List as defense articles: "Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality or information or information systems . . .").

[80] Items that possess a potential for use in both a commercial and military market.

[81] The EARs promulgate the policies set forth by the Export Administration Act of 1979. *See* 50 U.S.C. §§ 2401-2420 (1994), which lapsed on August 20, 1994; *see also* 15 C.F.R. § 768 (1997). Nonetheless, President Clinton issued an executive order requiring that the EAR be kept in force to 'the extent permitted by law' under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706 (1988 & Supp IV 1992). *See* Continuation of Export Control Regulations, Exec. Order No. 12924, 59 Fed. Reg. 43437 (1994). President Clinton recently extended the state of emergency required to activate his authority under IEEPA. *See* Continuation of Emergency Regarding Export Control Regulations, 61 Fed. Reg. 42527 (1996); *Planet Clipper*, *supra* note 12, at 21 n.20.

[82] *See* JAMES CHANDLER ET AL., REVIEW AND ANALYSIS OF U.S. LAWS, REGULATIONS, AND CASE LAWS PERTAINING TO THE USE OF COMMERCIAL ENCRYPTION

encrypting a message are listed on the USML unless the product is restricted to financial uses such as ATMs."[83]

The AECA authorizes the President to control the export of defense articles by designating such items on the USML.[84] While products governed by the EAR can be exported under a general license, encryption products falling under ITAR need a separate license application and review which ordinarily involves a referral to the Defense Department and the National Security Agency.[85] More specifically, "[o]nce on the USML, and unless otherwise exempted, a defense article or service requires a license before it can be imported or exported."[86] However, encryption products with key-lengths of more than 40-bits were generally not exportable.[87] It is not altogether clear why the level was set at 40-bits; howev-

---

PRODUCTS FOR VOICE AND DATA COMMUNICATIONS, (1994) *reprinted in* BUILDING IN BIG BROTHER 435, at 443 (Lance J. Hoffman ed., 1995) (Also included on the CCL are those cryptographic items involving message authentication, access control devices, television descramblers, automatic teller machines, virus protection, and "smart cards").

[83] *See Planet Clipper, supra* note 12, at 21.

[84] *See* 22 U.S.C. § 2778; *see also* 22 C.F.R. § 121.1 (United States Munitions List).

[85] *Planet Clipper, supra* note 12, at 21. *See also* Stewart Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions*, 452 PLI/Pat 287, 293 (Sept. 1996) [hereinafter *Baker FAQ*]. *See* Rubenstein, *supra* note 37, at 198 (noting that one of the stages of the approval process for encryption software is NSA Review). Rubenstein goes on to note that a "rule of thumb for encryption exporters is to . . . develop a good working relationship with the NSA." *Id.* NSA, in effect, is the only government agency with the technical expertise for evaluating whether cryptographic products fall within one category or another. *Id.*

[86] Bernstein v. United States Dep't of State, 922 F.Supp. 1426, 1429 (N.D. Cal. 1996). "The ITAR is administered primarily within the Department of State by the Director of the Office of Defense Trade Controls (ODTC), Bureau of Politico-Military Affairs." The ITAR allows for a 'commodity jurisdiction procedure' by which the ODTC determines if an article or service is covered by the USML when doubt exists about an item." 22 C.F.R. 120.4(a). Categories of items covered by the USML are enumerated at section 121.1 Category XIII, Auxiliary Military Equipment, includes "[C]ryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems . . . ." 22 C.F.R § 121.1 XIII(b)(1) (1997). A number of applications of cryptography are excluded, such as those used in automated teller machines and certain mass-marketed software products that use encryption. *Id. See also* 22 U.S.C. 2778(b)(2).

[87] *See Planet Clipper, supra* note 12, at 22-23 (*citing* U.S. Department of Commerce and National Security Agency, *A Study of the International Market for Computer Software With Encryption II-2* (1996). *See also Baker FAQ, supra* note 85, at 293 (noting that "the State Department routinely allows the export of cryptographic software

er, "[m]ost likely, it was the result of a set of compromises that were politically driven by all of the parties involved."[88]

Several regulations and statutes collectively authorized control of *all* cryptographic products and were administered by the Department of State and the Department of Commerce.[89] ITAR is a very restrictive export control regulation applying only to those items that the government considers most threatening to U.S. security interests.[90] The mere fact that cryptographic products were placed within ITAR's jurisdiction speaks volumes about the government's perception of the potential security risk that export of crypto presents. Controls on crypto products are designed to have a limiting effect on the further global proliferation of strong encryption.[91] Moreover, there can be little doubt that the ultimate goal of controls on crypto products is to "keep strong cryptography out of the hands of potential targets of signals intelligence."[92] The controls limit to a great extent the basic availability of encryption software of strategic and

---

that use algorithm with a key length of 40 bits or less, provided that stronger encryption cannot be easily substituted or installed").

[88] CRISIS, *supra* note 4, at 122.

[89] Export controls were even more onerous during the Cold War. During the Cold War, the United States was a member of the Coordinating Committee for Multilateral Export Controls (COCOM), which coordinated export regulations among the various members in an effort to prevent sensitive technologies from finding their way to the Eastern Bloc. "Under COCOM, any member could effectively veto the decision of another member to re-export a sensitive technology or product." However, with the fall of Russia and the Eastern Bloc, COCOM's purpose also disappeared, and it was formally dissolved in March, 1994. Sean M. Flynn, *A Puzzle Even The Codebreakers Have Trouble Solving: A Clash of Interests Over The Electronic Encryption Standard,* 27 LAW & POL'Y INT'L BUS. 217, 225-26 (1995).

[90] *See generally* Peter D. Trooboff, *A Brief ITAR Primer in the International Traffic in Arms Regulations (ITAR), in* COPING WITH U.S. EXPORT CONTROLS 1996, at 219-36 (PLI Comm. Law and Practice Course Handbook Series, 1996) (discussing how ITAR differs from other export control regimes and how exporters can comply with it).

[91] *See* ASSOCIATION FOR COMPUTING MACHINERY, INC., CODES, KEYS AND CONFLICTS: ISSUES IN U.S. CRYPTO POLICY 25 (June 1994) [hereinafter ACM] ("The goals of U.S. export control policy in the area of cryptography are (i) to limit foreign availability of cryptographic systems of strategic capability, namely, those capable of resisting concerted cryptanalytic attack; (ii) to limit foreign availability of cryptographic systems of sufficient strength to present a serious barrier to traffic selection or the development of standards that interfere with traffic selection by making the messages in broad classes of traffic (fax, for example) difficult to distinguish; and (iii) to use the export-control process as a mechanism for keeping track of commercially produced cryptosystems, whether U.S. or foreign, that NSA may at some time by called upon to break").

[92] CRISIS, *supra* note 4, at 128.

in many cases non-strategic value.[93] Additionally, export controls allow the National Security Agency (NSA)[94] to assess the quality of commercially available software.[95] But most importantly, export controls limit the availability of encryption products that could hinder efforts by NSA or various law enforcement agencies to obtain intelligence information.[96]

B. Current Control of Encryption Under EAR

In 1993, beginning with the Clipper chip initiative,[97] the Clinton

---

[93] *See* Charles L. Evans, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets,* 19 N.C. J. INT'L L. & COM. REG. 469, 488 (1994). *See also* CRISIS, *supra* note 4, at 127-34. Of course, regardless of which side one takes in the debate over whether these controls are in fact effective, it is a truism that any restrictions will limit availability to one extent or another. Consequently, the question then becomes one of relative impact effectiveness. *See id.* at 127-28.

[94] The National Security Agency, an intelligence agency generally considered more secret than the Central Intelligence Agency (CIA), is charged with both keeping our secrets and breaking theirs. *See* JAMES BAMFORD, THE PUZZLE PALACE (1982). The National Security Agency (NSA) is America's largest intelligence agency. The National Security Agency was established on October 24, 1952, by a top secret seven-page presidential memorandum signed by then-President Harry S. Truman. The Central Intelligence Agency (CIA), on the other hand, was established by public law, the National Security Act of 1947 (codified as amended at 50 U.S.C. §§ 401-432 (1994)). The Department of Defense, Secretary of Defense is responsible for directing, operating, and controlling the National Security Agency. *See* Exec. Order No. 12333, 46 Fed Reg. 59,941, 59,947 (1981). NSA is responsible for the "[e]stablishment and operation of an effective unified organization for signals intelligence activities . . . ." *Id.* at 59,947. NSA is charged with collection, processing and dissemination of signals intelligence information for national foreign intelligence purposes. *See id.* Additionally, NSA is responsible for the "[c]onduct of research and development to meet the needs of the United States for signals intelligence and communications security." *Id.* In short, NSA has a simple yet immense job – "to eavesdrop on the entire world, picking up all electronic transmissions, no matter how faint or what point of origin, then to plow through this pile of chaff to find the kernels of intelligence . . . ." ERNEST VOLKMANN & BLAIR BAGGET, SECRET INTELLIGENCE 178 (1989).

[95] *See* BAMFORD, *supra* note 94.

[96] *Id.*

[97] *See* CRISIS, *supra* note 4, at 170-74. "[T]he Clipper initiative was conceived as a way for providing legal access by law enforcement authorities to encrypted telephony. The Escrowed Encryption Standard (EES), a Federal Information Processing Standard (FIPS-185), was promulgated in February 1994 as the key technological component of the Clipper initiative . . . . Specifically, the EES called for the integration of special microelectronic integrated circuit chips (called "Clipper chips") into devices used for voice communications; these chips, as one part of an overall system, provide voice

Administration started down a long road of crypto controversy.[98] The essence of the Administration's encryption policy is predicated on the concept of "escrowed" encryption.[99] The Administration's crypto policy evolved through a number of incarnations.[100] However, current policy can trace its roots to Vice President Gore's statement of the Administration's policy on October 1, 1996.[101] This somewhat revised

---

confidentiality for the user and exceptional access to law enforcement authorities." *Id.* at 170-71. *See also* Dorothy E. Denning & Miles Smid, *Key Escrowing Today*, IEEE COMM. MAG., Sept. 1994, at 58, 58.

[98] *See supra* note 50 and accompanying text.

[99] *See supra* notes 34-38 and accompanying text for an explanation of escrowed encryption.

[100] *See Metaphor, supra* note 1, at 752-811 (outlining the evolution and details of various Clipper initiatives and escrowed encryption).

[101] The Clinton Administration's overall policy concerning the proliferation of strong encryption no doubt can be traced quite beyond Gore's Oct. 1 statement; however, the current incarnation of crypto policy really finds its basic form in the statement of the administrations objectives and concerns by Gore. Consequently, the succinct statement of policy by Vice President Gore is excerpted below.

> President Clinton and I are committed to promoting the growth of electronic commerce and robust, secure communications worldwide while protecting the public safety and national security. To that end, this Administration is consulting with Congress, the information technology industry, state and local law enforcement officials, and foreign governments on a major initiative to liberalize export controls for commercial encryption products . . . .
>
> Under this initiative, the export of 56-bit key length encryption products will be permitted under a general license after one-time review, and contingent upon industry commitments to build and market future products that support key recovery. This policy will apply to hardware and software products. The relaxation of controls will last up to two years . . . .
>
> The Administration's initiative recognizes that an industry-led technology strategy will expedite market acceptance of key recovery, and that the ultimate solution must be market-driven . . . .
>
> No key length limits or algorithm restrictions will apply to exported key recovery products.
>
> Domestic use of key recovery will be voluntary, and any American will remain free to use any encryption system domestically.
>
> The temporary relaxation of controls is one part of a broader encryption policy initiative designed to promote electronic information security and public safety . . . . The Administration also will seek legislation to facilitate commercial key recovery, including providing penalties for improper release of keys, and protecting key recovery agents against liability when they properly release a key . . . .

Clipper III policy proposed the "development of federal standards for key recovery, adoption of key recovery systems within the federal government, and liberalization of export controls for products that provide key recovery."[102]

> [The administration's] policy is designed to provide better encryption to individuals and businesses while ensuring that the needs of law enforcement and national security are met. Encryption is a law and order issue since it can be used by criminals to thwart wiretaps and avoid detection and prosecution. It also has huge strategic value. Encryption technology and cryptanalysis turned the tide in the pacific and elsewhere during World War II.[103]

Key recovery is, however, essentially about resolving a fundamental dilemma of encryption — that is, allowing the use of robust algorithms with long keys, while at the same time providing for code breaking under controlled conditions, for instance, by government officials with a court order.[104]

On December 30, 1996, the Clinton Administration implemented new regulations governing encryption.[105] These new measures include relaxing export controls for certain commercial encryption products, developing, in cooperation with industry, performance standards for a Key

---

> Two years from now, the export of 56-bit products that do not support key recovery will no longer be permitted. Currently exportable 40-bit mass market software products will continue to be exportable. We will continue to support financial institutions in their efforts to assure the recovery of encrypted financial information. Longer key lengths will continue to be approved for products dedicated to the support of financial applications . . . .
>
> The Administration's initiative is broadly consistent with the recent recommendations of the National Research Council. It also addresses many of the objectives of pending Congressional legislation.

The White House, Office of The Vice President, Statement Of The Vice President, Oct. 1, 1996 (statement by Vice President Gore on major initiative to liberalize export controls for commercial encryption and promote key escrow).

[102] *See Encryption Policy, supra* note 9.

[103] THE WHITE HOUSE, OFFICE OF THE VICE PRESIDENT, STATEMENT OF THE VICE PRESIDENT (Feb. 4, 1994), *reprinted in* BUILDING IN BIG BROTHER 235, at 235 (Lance J. Hoffman ed., 1995).

[104] *Id.*

[105] 15 C.F.R. pts. 730-774 (1997); Amendment to the International Traffic In Arms Regulations, 22 C.F.R. pt. 121 (1997). *See also* Felice Kaden Laird, *Summary Of Regulations Transferring Jurisdiction Over Commercial Encryption Products From State To Commerce,* THE EXPORT PRACTITIONER, 1/15/97 Export Prac. 4, *available in* 1997 WL 8530599. *See* Rubenstein, *supra* note 37, at 186-203 (providing comprehensive review of export controls on encryption products).

Recovery System, transferring export control jurisdiction of encryption from State to Commerce, and allowing a "trusted third party" hold the escrowed keys.[106] If companies agree to begin formulating a key-recovery system, they will be allowed to export non-recovery 56-bit key length strong encryption for up to two years.[107] In effect, the government will now allow companies to export stronger encryption products, "provided they have a plan to store 'spare keys' for unlocking encrypted information with a government-approved third party."[108] Additionally, encryption was transferred from the USML to the CCL of the EAR[109].

IV. CHALLENGES TO THE CONTROL REGIME

> The Administration needs to work with Congress to develop a consensus on a national encryption policy that takes account of the privacy, law enforcement and competitiveness concerns of out Nation's citizens and businesses.[110]
>
> — Senator Patrick Leahy

The crypto export control regime, long considered a national security given, is under attack, both in court and Congress. Attacks on crypto controls have come on two fronts, constitutional court challenges and legislative proposals in Congress.

The United States Congress has a number of bills before it with the goal of relaxing controls on the export of encryption.[111] There have been at least three significant cases presenting constitutional challenges to encryption licensing controls.[112] While congressional efforts appear to be motivated mostly by financial or international trade concerns, court

---

[106] *See* Laird, *supra* note 105.

[107] *See* I.J. Prior, *Controls on Cryptography Boil Down to Old Fashioned Politics*, 4/15/97 EXPORT PRAC. 6 (1997) *available in* 1997 WL 8530637.

[108] *See* Elizabeth Corcoran, *House Committee Approves Bill to Relax Curbs on Encryption*, WASH. POST, May 15, 1997, at E01. As of May 1997, 24 companies had applied for permission to export stronger encryption pursuant to the new regulations. About half the applications were approved. *See id.*

[109] 15 C.F.R. pts. 730-774 (1/7/97, supersedes 1/4/97). The interim rule amending EAR was published on December 30, 1996. *See* 61 Fed. Reg. 68572-68587 (1996). ITAR was amended at 61 Fed. Reg. 68633 (to be codified at 22 C.F.R. 121).

[110] *See Statement Of Senator Patrick Leahy (D-VT) On The Administration's New Encryption Initiative, (poted on* Oct. 1, 1996) (visited Mar. 12, 1998) <http://www.cdt.org/crypto/clipper311/961001_Leahy_stmnt.html> (urging Congress to address shortcomings of the Clinton Administration's plan for a national encryption policy).

[111] *See Showdown on Encryption, supra* note 73.

[112] *See* Fields, *supra* note 50, at 996-98.

challenges find their predicate on constitutional grounds. However, both seek the dismantling of the current control regime. Whether challenges are constitutional or congressional, national security is the government's primary response and, moreover, the crucial element of the equation. Export controls have been gradually loosened since 1983.[113] The question now is just how much further this relaxation can proceed without damaging national security.

A. Congressional Challenges to Crypto Licensing Controls

In the 105th Congress, legislation challenging the government's control of encryption technology has been introduced in both the House of Representatives and Senate.[114] Most of these proposals seek to take encryption issues out of political and national security spheres of influence and place them firmly within the commercial arena.[115]

Senator Conrad Burns (R-MT) has reintroduced legislation to eliminate export control of encryption technology.[116] Pro-CODE or "The Promotion of Commerce On-line in the Digital Era Act," generally allows for the unrestricted export of encryption products.[117] The bill requires allowing the export of encryption technologies if products of a similar strength are available elsewhere in the world and prohibits imposition of a mandatory key-escrow program.[118] The bill also prohibits the Com-

---

[113] *See* CRISIS, *supra* note 4, at 166.

[114] *See* Prior, *supra* note 107. However, most of the current legislative action originated during the 104th Congress, where a number of bills dealing with encryption technology were first introduced. *See generally Pro-CODE Hearings, supra* note 58 (transcribing Senate Committee Hearings on the Pro-CODE Act); S. 1726, 104th Cong. (1996) ("Promotion Of Commerce On-Line In The Digital Era (Pro-CODE) Act Of 1996"); H.R. 3011, 104th Cong. (1996) ("Security And Freedom Through Encryption (SAFE) Act"). However, none of these bills made it to the Senate or House floor for a vote before the end of the session. *See Encryption Policy, supra* note 9. Many of the bills currently before the 105th Congress are reintroductions of bills from the 104th Congress. *Id.*

[115] *See* Prior, *supra* note 107.

[116] *See* S. 377, 105th Cong. (1997). It is virtually identical to Burn's previous attempt to ban all export regulations relating to cryptography, S. 1726, 104th Cong. § 5(c) (1996). *See* Burns, *Burns Introduces Internet-Friendly Bill: "Pro-CODE" To Give Computer, Cell Phone Users Privacy, Security* (made available Feb. 27, 1997) <www.senate.gov/~burns/p-feb27.htm> [hereinafter *Internet-Friendly Bill*]. Senator Burns is the chairman of the Commerce Subcommittee on Science, Technology and Space.

[117] S. 377, 105th Cong. (1997).

[118] *Id.* For a summary of the specifics of the bill, see also *Bill Summary and Status Information, Digest, S 377* (visited Mar. 12, 1998) <http://thomas.loc.gov/cgibin/dquery105.html#blno>.

merce Department from imposing any encryption standards on the private sector.[119] There can be little mistake as to the intent of the bill. Senator Leahy (D-VT), a co-sponsor of Pro-CODE as well as sponsor of his own encryption legislation, states, "These bills . . . roll back current restrictions on the export of strong cryptography so that high-tech U.S. firms are free to compete in the global marketplace and meet the demands of customers — both foreign and domestic — for strong encryption."[120]

Pro-CODE is being paraded as promoting "electronic commerce through the use of strong encryption,"[121] but the question that must be asked is, at what expense and for what reason? Senator Burns believes that "online commerce will never reach its full potential under the policies of the [Clinton administration]."[122] Senator Burns sees the problem of encryption proliferation not in security terms, but strictly in dollar terms.[123] The Clinton administration opposes Burns' bill because "it does not balance the needs of individual privacy and economic growth with national security and public safety."[124]

Senator Patrick Leahy introduced the Encrypted Communications Privacy Act of 1997 on the same day that Senator Burns introduced his Pro-CODE bill.[125] Senator Leahy's bill generally mirrors Senator Burns' attack on crypto export controls, but also seeks protection of any U.S. person using encryption, regardless of strength, in any State or foreign country.[126] The bill also criminalizes the use of encryption when used in furtherance of a crime.[127]

Representative Bob Goodlatte (R-VA) introduced the Security and Freedom Through Encryption Act (SAFE).[128] SAFE relaxes crypto export controls on encryption products deemed generally available interna-

---

[119] *See* S. 377.

[120] *Encryption Bills Make Their Way Back to Capitol Hill,* COMMUNICATIONS TODAY, Feb. 28, 1997, *available in* 1997 WL 7465590.

[121] *See* S. 377.

[122] *Internet-Friendly Bill, supra* note 116.

[123] *See id.* ("Burns and supporters have pointed to a study that estimates a loss of $60 billion and more than 200,000 jobs to foreign competitors under current restrictions").

[124] Bill Pietrucha, *Burns, Leahy Introduce Encryption Export Legislation, Newsbytes,* (visited Nov. 3, 1997) <wysiwyg://13/http://www.nbnn.com/nbcgibin.udt/show.NB.NEW?ID=86898> (quoting Undersecretary of Commerce William Reinsch).

[125] S. 376, 105th Cong. (1997) (introduced, Feb. 27, 1997).

[126] *See id.* (proposing the enactment of § 2805 for the protection of U.S. nationals using encryption).

[127] *See id.* (outlawing both the use of encryption to obstruct justice and the unauthorized release of decryption keys).

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

tionally and prohibits the implementation of a mandatory key escrow regime. The bill provides the right to freely use any strength encryption product. And like the Pro-CODE bill, it creates new criminal penalties for using crypto in furtherance of a crime.

However, Senators John McCain (R-AZ) and Bob Kerrey (D-NE) have introduced legislation which amounts to a different sort of "challenge" to the control of crypto technology.[129] The Secure Public Networks Act of 1997 "is quite broad, including many provisions from a draft administration bill that was informally circulated, as well as some provisions from the Pro-CODE and SAFE bills."[130] The Secure Public Networks Act generally codifies the Clinton administrations current regulations governing export of encryption technology[131] but makes some effort towards relaxation of the controls by allowing a list of factors to be considered in evaluating applications for export licenses for strong encryption products not based on a key recovery system.[132] Kerrey's bill also establishes stiff penalties for use of crypto in furtherance of a crime, and provides incentives for domestic use of key-recovery or key-escrow systems.[133] Additionally, unlike other legislative efforts to decontrol crypto, Kerrey's bill contains a presidential power provision — whereby the president "may waive provisions of this act with a finding of danger to national security, public safety, economic security, or public interest."[134]

It is difficult to predict how any of these legislative proposals might fare in the coming months. There is some support for the SAFE and Pro-CODE bills, but it is unlikely that either one has enough support for passage at present, let alone enough to overcome a very predictable presidential veto. The Secure Public Networks Act is ostensibly an attempt at a compromise solution. However, it has not garnered much support at all from either the Pro-CODE or SAFE camps. Consequently, at least for the near term, export control of crypto is unlikely to fall at the hands of Congress.

It is difficult to predict how ant of these legislative proposals might fare in the coming months. There is some support for the SAFE and Pro-

---

[129] *See Net Tangle on Privacy*, WASH. POST, June 22, 1997 at C6 (Many would not consider the legislation a challenge at all, but rather an attempt to shore up recently relaxed controls.).

[130] Stewart Baker & Michael D. Hintze, *Government Regulation of Encryption*, 760 PLI/Comm 445, 453 (1997). *See also* S. 909, 105th Cong. (1997).

[131] *See id.* (allowing export of 56-bit crypto after one time review; export of stronger crypto if based on qualified system of key recovery).

[132] *Id.*

[133] *See id.*

[134] *Id.*

CODE bills, but it is unlikely that wither one has enough support for passage at present, let alone enough to overcome a very predictable presidential veto. The "Secure Public Networks Act" is ostensibly an attempt at a compromise solution; however, it has not garnered much support at all from either the Pro-CODE or SAFE camps. Consequently, at least for the near term, export control of crypto is unlikely to fall at the hands of Congress.

B. Constitutional Challenges to Crypto Licensing Controls

The U.S. Department of State, until most recently, was the primary gatekeeper for security export controls on crypto. Consequently, the State Department has received the full legal wrath of our modern-day crypto knights — those individuals so seemingly disenchanted with the apparently Orwellian-esque system that dares to challenge their "right" to be unheard.[135] In short, crypto security controls have been subject to a number of lawsuits in the past several years. These lawsuits have sought to challenge the underlying validity of the security export controls. Not so surprisingly, the primary weapon of choice for these crypto knights has been the First Amendment.

1. *Karn v. United States Department of State*[136]

---

[135] *See* Phillip E. Reiman, *Cryptography and the First Amendment: The Right to Be Unheard,* 14 J. MARSHALL J. COMPUTER & INFO. L. 325, 326-27, 334-37, 339-41 (1996) (arguing for analysis of cryptography as "undeniably a form of speech" and "not simply an extension of existing free speech concepts, but a new dimension of our constitutional rights").

[136] 925 F. Supp. 1 (D.D.C. 1996). Of note, on January 21, 1997, the D.C. Circuit Court of Appeals ruled on Karn's appeal of the district court decision. The appellate court remanded his case back to district court. The Court of Appeals chose to remand the case for reconsideration in light of the recent shift in crypto regulations from control by the State Department to the Commerce Department. Judge Richey, who originally considered and ruled against Karn, will consider the case most likely some time this spring. *See* Karn v. Department of State, No. 96-5121, 1997 WL 71750, at **1 (D.C. Cir.) ("In light of the recent Executive Order transferring regulatory authority of non-military cryptographic computer source code to the Commerce Department, and the Commerce Department's promulgation of a new regulation under the authority of the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 *et seq.*, we remand this case to the district court to consider the reviewability of and, if appropriate, the merits of appellant's claim under the Administrative Procedure Act. Because "basic tenets of judicial restraint and separation of powers call upon [the court] first to consider alternative grounds for resolution" when the court is asked to answer a question involving the Constitution of the United States (Lamprecht v. FCC, 958 F.2d 382, 389-90 (D.C. Cir. 1992)), we do not reach the constitutional issues

Phillip Karn filed suit against the government because the State Department would not allow him permission to export a floppy disk which contained a number of strong cryptographic schemes.[137] The State Department's Office of Defense Trade Controls ruled that the disk was subject to ITAR control and denied its export.[138] After being denied on appeal, Karn filed suit in the United States District Court for the District of Columbia challenging the designation of the computer disk containing crypto as a "defense article."[139] Judge Charles R. Richey issued summary judgment for the government. The court held that designation of the diskette containing the cryptographic source codes as a "defense article" was not subject to judicial review;[140] export regulations did not violate Karn's free speech rights, and export limitations did not violate due process.[141] In fact, Judge Richey in his opinion wrote at some length regarding his impression of the "merits" of *Karn:*

> This case presents a classic example of how the courts today, particularly the federal courts, can become needlessly invoked, whether in the national interest or not, in litigation involving policy decisions made within the power of the President or another branch of the government. The plaintiff, in an effort to export a computer diskette for profit, raises administrative law and meritless constitutional claims because he and others have not been able to persuade the Congress and the executive Branch that technology at issue does not endanger the national security. This is a "political question" for the two elected branches under Articles I and II of the Constitution.[142]

There can be little doubt that Judge Richey took what could only be

---

raised by this appeal").

[137] Karn v. United States Dep't of State, 925 F. Supp 1, 2-3 (D.D.C. 1996).

[138] *Id.* at 3.

[139] *Id.* at 4.

[140] *See id.* at 9-14 (explaining that the ITAR was content neutral and narrowly tailored to further the significant government interest of controlling the proliferation of cryptographic products). In fact, there has been at least one attempt by Congress to preclude all judicial review of Commerce Department export control decisions, as Karn seeks to challenge here. *See* The Omnibus Export Administration Act of 1995, 104th Cong. § 112 (1995) (the so-called "anti-crypto amendment" to Section 112 regarding Administrative and Judicial Review).

[141] *Karn*, 925 F. Supp. at 13.

[142] *Id.* at 2-3. "The government clearly has an interest in preventing the proliferation of cryptographic software to foreign powers, and the regulation of the export of the cryptographic software is a rational means of achieving that goal. The Court will not substitute its policy judgments for that of the President [citation omitted], especially in the area of national security." *Id.* at 13.

considered a deferential stance in rejecting Karn's challenge. Yet, as Richey plainly notes, there is a strong basis both in law and reason for such a ruling. While the judiciary rarely should be taken out of a fight because of a "lack of expertise" or unsupported assertions of separation of power conflict, this is just such a case where the courts simply do not belong. It is the nature of the question that should compel such deference by the courts[143] — that is, can a lone citizen, or profit-seeking company, using the judiciary as a conduit, challenge the government's determination, which is supported by regulations and laws passed by Congress and enforced by the Executive, of what constitutes an external threat to U.S. security, arguably the most fundamental and significant of all governmental functions, essentially threat assessment? Karn stands for the proposition, simply put, that there must be some things that remain beyond judicial reproach, national security export controls being one of them.

2. *Bernstein v. United States Department of State*[144]

While *Karn* presented the cryptographic community with what could be referred to as a status quo ruling, *Bernstein* took quite another path when faced with a similar constitutional challenge.[145] The case began in 1995 when Daniel Bernstein, a then-graduate student in mathematics at the University of California at Berkeley, brought suit against the Depart-

---

[143] *See* Hayden v. National Security Agency, 608 F.2d 1381, 1388 (D.C. Cir. 1979) (upholding National Security Agency's determination of what constitutes a threat to national security interests, in the face of a FOIA request for classified information relating to foreign signals intelligence collection, as being "the sort of situation where Congress intended reviewing courts to respect the expertise of an agency").

[144] 945 F. Supp. 1279 (N.D. Cal. 1996).

[145] The ruling could be referred to as "status quo" in the sense that it gave preeminence or maximum deference to national security considerations when responding to a question involving the export of encryption technology, only until most recently considered "munitions" by the Defense Department. *See* CRISIS, *supra* note 4, at 4 ("For many years, concern over foreign threats to national security has been the primary driver of a national cryptography policy that has sought to maximize the protection of U.S. military and diplomatic communications while denying the confidentiality benefits of cryptography to foreign adversaries through the use of export controls on cryptography and related technical data"). Yet, the result and notably the level of deference was markedly different in Berstein. *See, e.g.*, 945 F. Supp. 1279, 1288 ("Under such an exacting standard, defendants' interest here, in being able to break foreign encryption and conduct adequate surveillance in furtherance of world peace and the security and foreign policy of the United States, 22 U.S.C. § 2778(a)(1), are clearly insufficient without more").

ment of State. Bernstein sought declaratory and injunctive relief from enforcement of the AECA[146] and ITAR,[147] as unconstitutional on their face and as they applied to him.[148]

In a preliminary ruling on the government's motion to dismiss for lack of justiciability, Judge Marilyn Patel held that cryptographic source code was protected First Amendment "speech" and that constitutional challenges to AECA and ITAR were justiciable.[149] In denying the government's motion to dismiss, Judge Patel found that the plaintiff was not seeking judicial review of the government's commodity jurisdiction determination, which classified the software as a "defense article" under ITAR and the USML;[150] rather, plaintiff was merely seeking to challenge the constitutionality of the statute and the regulations itself, which were justiciable.[151] Thus, this court became the first court to recognize a protected speech interest in computer code,[152] and the issue was transformed from the realm of the government's interest in controlling the export of material deemed harmful to national security, or a "political question" in *Karn*, to the right to speak cryptographically in *Bernstein.*

In *Bernstein II,* Judge Patel, facing cross-motions for summary judgment, held that licensing requirements under AECA and ITAR constituted unlawful prior restraint of cryptographic speech,[153] and that national security, standing alone, did not justify the restraint, even if the requirements were content neutral.[154] The court, citing *New York Times Co. v. United States,* found "national security, without more, too amorphous a rationale to abrogate the protections of the First Amendment."[155] The court noted, and as Justice Stewart's separate opinion in *New York Times* stated, that prior restraint is justified "only when disclo-

---

[146] *See* 22 U.S.C. § 2778.

[147] 22 C.F.R. §§ 120-130 (1997).

[148] *See* Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1428 (N.D. Cal. 1996).

[149] *See Bernstein,* 922 F. Supp. 1426, 1439 (N.D. Cal. 1996).

[150] *See* 22 U.S.C. § 2778(a)(1). "Once on the USML, and unless otherwise exempted, a defense article or service requires a license before it can be imported or exported," which in Bernstein's case made it a dead-letter. *Bernstein,* 922 F. Supp. at 1429.

[151] *See Bernstein,* 922 F. Supp. at 1431.

[152] *See* Thinh Nguyen, *Cryptography, Export Controls, and the First Amendment, in* Bernstein v. United States Department of State, 10 HARV. J.L. & TECH. 667, 672 (1997).

[153] *See Bernstein,* 945 F. Supp at 1290, 1292.

[154] *See id.* at 1288.

[155] *Id. (citing* New York Times Co. v. United States, 403 U.S. 713, 730 (Black, J. and Douglas, J. concurring).

sure would 'surely result in direct, immediate, and irreparable damage to our nation or its people.'"[156] Judge Patel further stated, "[u]nder such an exacting standard, defendants' interests here, in being able to break foreign encryption and conduct adequate surveillance in 'furtherance of world peace and the security and foreign policy of the United States,' 22 U.S.C. § 2778(a)(1), are clearly insufficient without more."[157]

Judge Patel's decision amounted to summary execution of controls on the proliferation of strong crypto. Patel dismissed the political question doctrine out of hand, quite in favor of a convoluted theory of cryptography as pure speech and not a technology that transforms communication between parties and makes no original speech expression in and of itself. The political question doctrine has a rich history and cannot be put to rest with a mere slight of the hand.[158] Moreover, declaring crypto or computer source code to be pure speech rather than conduct is highly problematic.[159] "It is particularly ill-suited to the realities of computer technology because software inseparably incorporates elements of both expression and function."[160] First Amendment protections for pure

---

[156] *Id.* (*citing* New York Times Co. v. United States, 403 U.S. at 730 (Stewart, J. and White, J. concurring).

[157] *Id.*

[158] *See generally* Baker v. Carr, 369 U.S. 186, 246 n.3 (1962) (discussing the situations in which the political question doctrine is applicable as including situations where discretion rests properly in the hands of the executive or legislative branches). Clearly, courts should and typically do consider constitutional questions that involve issues of national security. *See* New York Times Co. v. United States, 403 U.S. 713, 718-19 (1971) (involving an injunction against the publication of policy papers regarding the Vietnam Conflict). That is simply not in dispute. However, political questions regarding the export of materials, as in this case with strong encryption, which arguably possesses the ability to significantly alter the capacity of the U.S. intelligence community to make timely and accurate assessments of potential national security risks, are plainly not within the same sphere as publishing the Pentagon Papers. *See also* United States v. Mandel, 914 F.2d 1215, 1223 (9th Cir.1990) ("[W]hether the export of a given commodity would make a significant contribution to the military potential of other countries . . . is a political question not subject to review to determine whether [it] had a basis in fact"). There is little doubt that the President possesses the requisite power to evaluate what actually constitutes a valid "national security risk." *See* United States v. Curtiss-Wright Corp., 299 U.S. 304, 319-20 (1936) (finding inherent power over national security matters vested in office of President by virtue of constitutional authority in foreign relations).

[159] *See* Nguyen, *supra* note 152, at 675-79. "The problem with the court's analysis is that it focuses too narrowly on the nature of computer source code, rather than looking to the larger social context surrounding the regulated activities in which software plays a part." *Id.* at 677.

[160] *Id.* at 675-76.

speech are justifiably far-reaching; however, crypto is hard pressed to fall within those protections because it lacks the expression needed to invoke those protections.[161] Crypto is a technological device for passing information, not expression of pure speech. "A critical insight into the First Amendment protections of speech is that it attaches not to particular things or types of objects (such as computer source code) but to activities where the free exchange of information and ideas is at stake (such as publishing and giving a speech)."[162]

3. *Junger v. Christopher*[163]

A third suit has been filed by Peter D. Junger, a professor of law at Case Western Reserve University School of Law in Cleveland, Ohio, in U.S. District Court for the Northern District of Ohio.[164] Professor Junger is seeking an injunction and declaratory relief against enforcement of certain provisions of ITAR which seek to regulate the export of cryptographic devices, data, and information.[165] In short, he believes that ITAR

---

[161] *Id.* at 675-79.

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

[163] *See* Plaintiff's Brief, Junger v. Christopher, No. 1:96 CV 1723 (N.D. Ohio, filed Aug. 7, 1996) (all documents relative to this suit can be found on Professor Junger's homepage *available at* <http://samsara.law.cwru.edu/>). Junger, while uneventfully including as defendants the Secretary of State and the Director of State's Office of Defense Trade Controls (ODTC), Bureau of Politico-Military Affairs, agencies which ostensibly administer the ITAR, made the additional and somewhat curious step of including Lt. General Kenneth A. Minihan, Director of the National Security Agency (NSA) as a defendant in his suit. *See* Complaint, Junger v. Christopher, No. 1:96 CV 1723 (N.D. Ohio, filed Aug. 7, 1996). Although it is well-known that the State Department "consults" NSA before it approves or denies (or more probably even whispers the word cryptography) anything, and in effect NSA has the final word on crypto-ITAR questions, it had been, at least until present, implicitly considered somewhat taboo, and likely the kiss of death, to include NSA as a defendant in any suit. *See* William Tanenbaum, *Computer Security and Encryption (In the Form of Frequently Asked Questions), in* MULTIMEDIA 1997: PROTECTING YOUR CLIENT'S LEGAL AND BUSINESS INTERESTS (available in WESTLAW, 467 PLI/PAT 575, 589) ("In practical effect, the National Security Agency has de facto control over the issuance of export licenses because the Department of State will not grant a license without NSA approval").

[164] *See* Michele Fuetsch, *Professor Fights U.S. On Encryption,* PLAIN DEALER, Aug. 8, 1996, at B1.

[165] *See* PRESS RELEASE, PLAINTIFF SEEKS SUMMARY JUDGMENT IN CLEVELAND CASE CHALLENGING LICENSING OF EXPORTS OF CRYPTOGRAPHIC INFORMATION (Attorneys Raymond Vasvari & Gino Scarselli, Oct. 1, 1996) (last visited Nov. 10, 1997) <http://samsara.law.cwru.edu/comp-law/juc/pressrel2.html>.

as it applies to crypto is unconstitutional because they deprive him of his First Amendment right to academic freedom.[166] Specifically, Professor Junger alleges claims of prior restraint, overbreadth and vagueness, restrictions on academic and political speech, freedom of association, and inference with a separation of powers.[167]

It is important to note that unlike the arguments in *Bernstein* and *Karn,* Junger does not, per se, challenge the constitutionality of requiring one to get a license before exporting a physical cryptographic device. However, requiring the permission of the government before one can communicate knowledge is, in the words of Junger, unconstitutional. Junger further claims that "[s]uch a prior restraint is, in fact, the paradigmatic example of a violation of the First Amendment."[168]

The crux of Professor Junger's claim against the State Department (and of course NSA) results from a strict reading of the ITAR provisions regarding what precisely constitutes an "export."[169] ITAR, of course, is, by effect and design, sweeping in impact.[170] Generally, ITAR prevents disclosure of all crypto information, data, or performance of defense services[171] related to prohibited crypto.[172] Professor Junger's concern

---

[166] *See id.*

[167] *See* Complaint at ¶ 32-70, Junger v. Christopher (No. 1:96 CV 1723).

[168] *See* PRESS RELEASE, *supra* note 165.

[169] *See* 22 C.F.R. § 120.17 (1997) (An "export" under ITAR: "sending or taking a defense article out of the United States in any manner," *id.* § 120(a)(1), "disclosing (oral or visual) or transferring technical data to a foreign person whether in the United States or abroad," *id.* § 120.17(a)(4), "performing a defense service on behalf of, or for the benefit of, a foreign person," *id.* § 120.17(a)(5).). Of note, Professor Junger's concern regarding exposure of ITAR regulated crypto to "foreign persons" is by no means unheard of, as it has consistently been a serious concern with American businesses, which use crypto both here and abroad, employing foreign nationals for work in the U.S. and abroad. Mostly these "exports," though, would be inadvertent. *See Baker FAQ, supra* note 85, at 298-300. Junger, however, intentionally wants to disclose ITAR-regulated matter.

[170] Remember, of course, ITAR's purpose is to regulate the export of items, data, devices, or information considered by the government potentially to have an adverse impact on national security. *See supra* notes 78, 79, 90 and accompanying text.

[171] Section 120.9 defines "defense services" as furnishing of assistance to foreign persons with respect to defense articles or the furnishing of technical data to foreign persons, in the U.S. or abroad. 22 C.F.R. § 120.9 (1997).

[172] *See* 22 C.F.R. pts. 123-25. Under ITAR, all crypto that comes within its somewhat murky domain requires special licensing and approval. As notes 87-88 explain, anything over 40-bits is routinely denied, unless it falls under prescribe exceptions, such as use in financial networks or used for authentication purposes. Consequently, as Professor Junger correctly asserts, disclosure to a foreign person, here or abroad, of "prohibited" crypto would violate ITAR, save obtaining a license, which

is that he might violate ITAR if he discloses ostensibly ITAR-regulated cryptographic software and technical data to foreign persons, in the course of his duties as a law professor. He also wishes to publish course materials and articles containing this same sort of cryptographic information.[173] Moreover, Junger believes that he should freely be able to send his "materials" abroad without regulation and licensing by the State Department.[174] In particular, Professor Junger asserts in his Complaint,

> By requiring registration and a license prior to the disclosure of unclassified cryptographic software or cryptographic technical data within the United States, the defendants are engaged in controlling the exchange of cryptographic information between persons within the United States, including the dissemination of cryptographic information on the Internet. The defendants have therefore adopted a *de facto* policy of restricting the domestic dissemination of unclassified cryptographic information which has the direct effect of restricting the availability of cryptographic software within the United States.[175]

Professor Junger, in short, challenges the constitutional validity of a regulation which not only seeks to restrict the dissemination of crypto beyond U.S. borders, but has the indirect effect of restricting his speech and conduct within the U.S. with respect to crypto.

Clearly, his argument is novel and should be closely watched.[176] However, it is likely that, if anything, the public domain exception will either be re-crafted or interpreted in such a way as to allow Professor Junger to disseminate his materials in the classroom before any court finds ITAR unconstitutional on the grounds asserted by Professor Junger.[177]

---

is arguably not only impractical but likely impossible.

[173] *See* Complaint at ¶ 1, Junger v. Christopher (No. 1:96 CV 1723).

[174] *See id.*

[175] *See id.* ¶ 64.

[176] Professor Junger has filed a revised complaint in light of recent changes to the regulations controlling crypto.

[177] Ostensibly, the "public domain" exception to ITAR provides the necessary "out" for Professor Junger's concerns. *See* 22 C.F.R. § 120.11 (1997) ("information which is published and which is generally accessible or available to the public . . . "). However, as some commentators have noted this appears to exempt from controls only "information" and not "data" (including software), which Junger also seeks to "export." *See* Ira S. Rubinstein, *Export Controls on Encryption Software, in* COPING WITH U.S. EXPORT CONTROLS 1995, at 401, 410 (PLI Comm. Law and Practice Course Handbook Series, 1995).

C. The Essence of the Debate Over Strong Crypto

> As we move into the twenty-first century, we must provide our law enforcement and national security officials with the tools that they need to do their jobs in the Information Age. The issue . . . centers upon a technology that some claim makes the jobs of law enforcement, national security, and armed services more difficult. However, governmental policy regulating this technology is beginning to pose some very serious commercial concerns.[178]

There is little question that enormous advances in telecommunications in the fifty years have created the opportunity for public use of encryption to ensure the privacy and integrity of business and personal communications.[179] However, at the same time, these same advances seriously threaten the capabilities of law enforcement and intelligence agencies to intercept a broad range of signal intelligence[180] targets, for instance, narcotraffickers, organized crime, terrorists, and foreign espionage agents.[181] Diverse interests are in diametric opposition to each other: industry's right to sell and the public's right to use crypto versus the government's duty to protect.[182]

Law enforcement and national security intelligence communities argue that if unmitigated proliferation of strong crypto is allowed, criminals, terrorists, and foreign intelligence targets of interest will not only evaporate, but eventually disappear entirely, which would in turn seriously compromise the government's ability to protect the security of the State and the safety of its citizens.[183]

Opponents of controls on the proliferation of crypto, on the other hand, contend that the public has a right to and expectation of crypto-enhanced privacy, strong privacy.[184] They argue that the criminals and spies have plenty of other crypto available worldwide, and therefore there

---

[178] *Online Encryption Technology: A Bill to Loosen Restrictions, supra* note 10 (statement of Chairman Sen. John McCain).

[179] *See* Lance J. Hoffman, *Afterword* to BUILDING IN BIG BROTHER 549 (Lance J. Hoffman ed., 1995) (quoting a May 3, 1993 Memo to the U.S. Deputy Sec. of Defense from Charles A. Hawkins, Jr., Acting Assistant Secretary of Defense (C3I)).

[180] Signals Intelligence (SIGINT) is a category of intelligence information comprising of communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). *See infra* note 220 (defining terms).

[181] *See* Hoffman, *supra* note 179, at 549.

[182] *See id.*

[183] *See id.*

[184] *See id.*

is simply no need to restrict U.S.-built crypto.[185]

> [Moreover], the computer industry points out that it has one of the few remaining positive trade balances and that it is vital that the dominance of the American computer industry in world markets be preserved. The industry fears that this will be lost if offshore developers incorporate high-quality cryptography into their products while U.S. industry either cannot do so or suffers higher costs or delays due to requirements for export licenses because of strict controls of export of cryptography.[186]

Of course, the government does not deny the importance of strong encryption to U.S. companies and private citizens alike.[187] Indubitably, encryption products both serve to protect proprietary data of U.S. companies worldwide[188] and have the *potential* to be an economic boom in the cryptography software market.[189] Obviously, the problem is reconciling all of these competing interests and sorting out the extremes, which are numerous, but without compromising any one interest too much. If that sounds impossible, then maybe it is.

---

[185] *See id.*

[186] *Id.*

[187] *See* The White House, Office Of The Vice President, Statement Of The Vice President, Oct. 1, 1996 (stating that "[t]he Administration's initiative recognizes that an industry-led technology strategy will expedite market acceptance of key recovery, and that the ultimate solution must be market-driven."); *see also* Text of a Letter From President To The Speaker Of The House Of Representatives And The President Of The Senate (visited Nov. 15, 1996) <http://www.law.miami.edu/%7Efroomkin/nov96-regs.htm> (stating that "because of the increasingly widespread use of encryption products for the legitimate protection of the privacy of data and communications in nonmilitary contexts; [and] because of the importance to U.S. economic interests of the market for encryption products . . . [encryption products will no longer be designated as defense articles on the U.S. Munitions List]).

[188] *See* ACM, *supra* note 91, at 1 (noting that in the 1970s, thousands of phone conversation that were conducted on IBM's private microwave network by IBM executives concerning business were "systematically eavesdropped upon by Soviet intelligence agents").

[189] *See* Evans, *supra* note 93, at 480 (arguing that the software industry is one of the fastest growing industries in the United States, and as the demand for software increases, so too will the demand for security-related products such as encryption software). *But see* ACM, *supra* note 91, at 12 (noting that "cryptography remains a niche market in which (with the exception of several hundred million dollars a year in government sales by a few major corporations) a handful of companies gross only a few tens of millions of dollars annually"). The fervent supporters of a wide-open, and profitable, cryptography market have prophesied for almost twenty years an explosion in the market. *Id.* In fact, in 1978 Whitfield Diffie, inventor of public key cryptography, "predicted that it would become ubiquitous by the mid-1980s." *Id.* at 13 n.6.

This, in a nutshell, is the cryptographic policy debate.[190]

V. THE NATIONAL SECURITY PERSPECTIVE

> The Necessity of procuring good Intelligence is apparent and need not be further urged—all that Remains for me to add is, that you keep the whole matter as secret as possible For upon Secrecy, Success depends in Most Enterprises of the kind, and for want of it, they are generally defeated, however well planned & promising a favorable issue.[191]
>
> — George Washington

Despite the potential economic benefits of decontrolling cryptography, decontrol also presents a number of compelling threats to national security. Opposition to further proliferation of strong encryption is predicated on a basic assumption—that wide-spread use of unbreakable cryptography is, to put it very mildly, not such a good thing. While it is recognized that a significant number of encryption programs are already available from non-U.S. sources worldwide, and in many cases obtained quite cheaply and easily,[192] it would appear not to be in the best interests of the United States, as a pure security matter, to contribute to the proliferation of encryption. This would be much as the United States chooses in many cases to restrict the export of other military-related technology that is also available from other sources.[193] Should the United States allow the export of sophisticated missile technology, just because it just so happens that the Chinese and the Russians have similar systems available on the open-market? That seems absurd, but it is exactly what opponents

---

[190] There are, of course, myriad of arguments against some or any controls on strong encryption. There is the economic argument that U.S. export controls threaten the U.S. software industry's ability to compete in foreign markets. *See, e.g.*, Evans, *supra* note 93, at 488-90. Dovetailing with that is the argument that key escrow will also stifle competitiveness because nobody would want to buy a product with a U.S. government back-door built into it. Additionally, probably the most prominent of crypto decontrol arguments concerns issues of privacy and the First Amendment. *See Metaphor, supra* note 1, at 812-21.

[191] George Washington, writing to a friend in 1777, *reprinted in* SECRET INTELLIGENCE, at xv (1989).

[192] *See Metaphor, supra* note 1, at 748 (arguing that U.S. export regulations designed to prevent the proliferation of strong encryption have generally failed). *See also Encryption Policy, supra* note 9 (noting that as of June 1996, Trusted Information Systems identified 1262 encryption programs worldwide from 68 countries; of these 730 were produced or distributed in the U.S.; the remaining 532 were of foreign origin).

[193] U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, EXPORT CONTROLS AND NONPROLIFERATION POLICY O.T.A.-ISS-596, 56 (1994) (noting that arguing for decontrol of exports because they can be found elsewhere is analogous to allowing uncontrolled gun sales to criminals simply because they can get them anyway).

of controls are arguing. Why help an already bad situation get worse?

A. No More Secrets

The phrase "No More Secrets" is a cryptic reference to the "little black box" device that forms the essential plot component for the film *Sneakers*.[194] The film presents an interesting problem: what if there were a device which could decrypt *any and all* encryption. That is, what if there were *no more secrets*, at least for the fortunate holder of the device. It is not hard to imagine that such a device would be enough to kill for, as the plot of the movie no doubt suggests.[195] But what does this have to do with the proliferation of strong crypto? Imagine the inverse of "no more secrets," that is, "too many secrets." What would be the impact to U.S. national security if strong encryption were abundantly available to terrorists or organized crime elements?[196] Security invariably would be compromised — *too many secrets*.[197]

---

[194] *See* SNEAKERS (Universal 1992) (starring in addition to Robert Redford, most notably, are Sidney Poitier, Dan Akroyd, River Phoenix, and Ben Kingsley). The film's plot involves Redford and his high-tech surveillance team, a sort of a 90's version of the *Dirty Dozen* (that is, mostly a group of misfits, ex-spooks, and computer geniuses), battling the forces of evil, represented by the former 60's student radical turned Mafia "accountant"/information systems manager, Ben Kingsley, who incidentally has obtained a black box which has the capability to decrypt any and all encryption schemes. In the film, Redford uses a Scrabble board to decrypt the ostensible "cover" name for the little black box, SETEC Astronomy – which breaks out to be, "too many secrets." Upon reaching this discovery, River Phoenix emphatically says, "So it is a code breaker?" Redford replies in an ominous tone, "No, it is *the* code breaker . . . no more secrets."

[195] *Id.* (Sidney Poiter: "There isn't a government on this planet that wouldn't kill us all for that thing").

[196] The point of this scenario is not to suggest that some form of strong crypto is not available at any given moment worldwide, as it is. Rather, the point is that just because something is available, for example, nuclear weapons, does not necessarily mean that a country should export their "wares."

[197] *See Online Encryption Technology: A Bill to Loosen Restrictions, supra* note 10 (statement of William P. Crowell, Deputy Director, National Security Agency) (noting that "if we overemphasize the public interests, we risk a world with too much government access and *too few secrets* . . . [while] if we overemphasize the interests of the private sector, we risk a world with perhaps *too many secrets* — for example, a world in which terrorists, organized crime, and hackers acquire the capability to operate with impunity") (emphasis added).

B. Threat or Perceived Threat?

> The world isn't run by weapons any more, or energy or money; it's run by little ones and zeros, little bits of data. Its all just electrons. . . there's a war out there old friend, a world war, and it's not about who's got the most bullets; its about who controls the information, what we see and hear, how we work, what we think; its all about the information.[198]

Those in favor of relaxation of control on encryption, typically software executives with a less than objective view, in other words, a serious eye on potential "profits,"[199] lament often and loudly about the "economic national security" of the United States.[200] The traditional national security threat is often presented with a certain cavalier attitude.[201] However, opponents of national security export controls often miss the fundamental point, and quite obviously misunderstand the nature of signals intelligence collection.[202] It clearly serves their interest to present

---

[198] *See* SNEAKERS (Universal 1992) (Ben Kingsley).

[199] This, by no means, is the only "pro-proliferation" group. As discussed in Section III B, there are serious constitutional questions regarding controls on strong encryption that have yet to be completely resolved. Those challenging controls on encryption in a constitutional context can be considered "pro-proliferation," to some extent. However, it is important to understand that the labels are ultimately unimportant. What is important, and what this and the following sections address, is whether the invocation by the current Administration of what is essentially a trump card — "a national security threat," warrants more than the perfunctory dismissal it has generally been given by the pro-proliferation group. National security is an inherently nebulous concept. Therefore, for the national security perspective to maintain a significant position within the debate over controls, some effort at explaining it within the context of cryptography must be undertaken. Whether the *level* of threat is in fact substantial, significant or compelling enough to *overcome* (trump) challenges, constitutional or otherwise, to controls on strong encryption is not within the design of this Note. Rather, this Note seeks only to explain the national security threat perspective and advocate a balancing of all significant interests.

[200] That is, the competitiveness argument that the U.S. software industry cannot compete abroad if they cannot export strong crypto in their products. In actuality, encryption software currently accounts for about one to three percent of the total software market. *See A Study of the International Market for Computer Software with Encryption*, U.S. Dept. of Commerce and the National Security Agency, Washington, D.C., 1996.

[201] *See, e.g.*, Judge Patel's decision in Bernstein v. United States Department of State, 945 F. Supp. 1279, 1288 (N.D. Cal. 1996).

[202] *See* Steven Levy, *The Cypherpunks vs. Uncle Sam*, N. Y. TIMES, June 12, 1994, § 6, *reprinted in* BUILDING IN BIG BROTHER 266, at 268 (Lance J. Hoffman, ed.,

the national security issues in a one-dimensional manner.[203] However, it is important not to misjudge or misstate the potential of the threat in the race to solve this prickly problem. "The government [clearly] understands the impossibility of eradicating strong crypto. [Rather], its objective is to prevent unbreakable encryption from becoming routine."[204] Because if that happens, even the dumbest and poorest criminals and terrorists in the world would have automatic extreme privacy for their criminal acts.[205]

Dorothy E. Denning, a Georgetown University computer scientist who is very active in the crypto debate, writes, "[a]ll communications on the information highway would be immune from lawful interception. In a world threatened by international organized crime, terrorism and rogue governments, this would be folly."[206] Additionally, Denning writes, "[w]e would have havoc in the United States . . . . Lawlessness would prevail."[207] If Denning is even marginally correct, crypto cannot, as some would have it, go uncontrolled. FBI Director Louis Freeh has testified before the Commerce Committee that if export controls were weakened without providing for a key-escrow system, national security

---

1995). Stewart A. Baker, former general counsel to NSA, explains the fundamental misunderstanding, "[t]he concern is not so much what happens today when people go in and buy voice scramblers; it is the prospect that in 5 years or 10 years every phone you buy that costs $75 or more will have an encrypt button on it that will interoperate with every other phone in the country and suddenly we will discover that our entire communications network is being used in ways that are profoundly antisocial. That's the real concern . . . . If we are going to have a standardized form of encryption that is going to change the world, we should think seriously about what we are going to do when it is misused." *Id.* at 272-73. Although Mr. Baker's comments ostensibly deal with "domestic security," his observations are, given the current atmosphere in world affairs and terrorism, applicable to national security in general.

[203] *See, e.g., Pro-CODE Hearings, supra* note 58 (testimony of Barbara Simons, Chair, U.S. Public Policy Committee of the Association of Computing Machinery).

> We recognize that the government has a legitimate interest in protecting national security. However, the government's proposals are becoming increasingly difficult to achieve as strong encryption programs are available and extensively used worldwide. Whether the U.S. Government keeps current export controls in place, or attempts to impose restrictions even on domestic use of encryption, the role of the national security agencies will remain difficult. Thus, we suggest that a policy which serves the long term interests of our nation's security will not be one based on key escrow, but rather one that anticipates the widespread availability of strong encryption.

Id. at 115.

[204] Levy, *supra* note 202, at 272.

[205] *Id.*

[206] Dorothy Denning, *The Clipper Chip Will Block Crime*, NEWSDAY, Feb. 22, 1994. (*quoted in* Luke Seemann, *Keys to Secret Drawers*, also available (visited Sept. 29, 1996) <www.stardot.com/~lukeseem/j202/essay.html>.

[207] *Id.*

would be at risk.[208]

> Previously, control of the availability and use of cryptography was presented as a national-security issue focused outward, with the intention of maintaining a U.S. technological lead over other countries. Now, with an increasing policy focus on domestic crime and terrorism, the availability and use of cryptography has also come into prominence as a domestic-security, law-enforcement issue. More widespread foreign use of cryptography — including use by terrorists and developing countries — makes U.S. signals intelligence more difficult. Within the United States, cryptography is increasingly portrayed as a threat to domestic security (public safety) and a barrier to law enforcement if it is readily available for use by terrorists or criminals. There is also growing recognition of the potential misuses of cryptography, such as by disgruntled employees as a means to sabotage an employer's databases. Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives intended to preserve U.S. law-enforcement and signals-intelligence capabilities.[209]

In fact, the traditional boundaries between "law enforcement" and the "intelligence community" have substantially blurred since the end of the Cold War.[210] Control of the availability and use of crypto has typically been presented as a purely "national security" issue, "focused outward, with the intention of maintaining a U.S. technological lead over other countries and preventing encryption devices from falling into the 'wrong hands' overseas."[211] U.S. crypto policy focused outward because the greatest threat appeared, and in fact was for a long time, outward — that is, widespread foreign use of strong encryption products and use by terrorists or developing countries potentially makes U.S. signals intelligence collection, an already difficult proposition, even more difficult still.[212] But in the last ten years, due to budget constraints and a significant increase in domestic terror crimes, often originating outside the United States, the availability or proliferation of encryption technology

---

[208] *FBI Says Senate Encryption Bill Could Jeopardize National Security*, COMMUNICATIONS TODAY, July 26, 1996, *available in* 1996 WL 10162133.

[209] U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS, 9-10 (1994).

[210] *See* Philip B. Heymann, *Law Enforcement and Intelligence in the Last Years of the Twentieth Century*, 18 NAT'L SEC. L. REP. 1 (Winter 1996).

[211] U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, ISSUE UPDATE ON INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 7 (June 1995).

[212] *See id.*

has become a domestic-security/law enforcement issue.[213] Strong encryption, therefore, can be perceived as a potential threat to the *fundamental* security of the United States, which effectively brings issues concerning domestic security firmly within the envelope of national security.[214] "Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives, like key-escrow encryption, that are intended to preserve U.S. law enforcement and signal-intelligence capabilities."[215] It is with this fundamental breakdown of the traditional dichotomy between intelligence and law enforcement in mind that the domestic security factoris discussed along with issues concerning the intelligence community in the sections that follow.

1. Impact on Foreign Signals-Intelligence Collection[216]

> Intelligence organizations provide the foreknowledge to the national leadership ("the princes")[217] and military commanders ("the generals")[218] by gathering intelligence information from a myriad of sources, evaluating this information to determine accuracy, analyzing the information from all available sources, and finally producing and dissemination an intelligence product or report to the consumer.[219]

The ability to intercept and exploit foreign signals intelligence[220] is

---

[213] *See id.*

[214] *See id.*

[215] *Id.*

[216] Intelligence is the "product resulting from the collection, evaluation, analysis, integration, and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediate or potentially significant to the development and execution of plans, policies, and operations." DEPARTMENT OF DEFENSE, *supra* note 30, at 175.

[217] A reference to Sun Tzu's "princes." *See supra* note 2 and accompanying quotation.

[218] A reference to Sun Tzu's "generals." *See supra* note 2 and accompanying quotation.

[219] David L. Christianson, *Signals Intelligence, in* THE MILITARY INTELLIGENCE COMMUNITY 39, 39 (Gerald W. Hopple and Bruce W. Watson eds., 1989).

[220] Signals intelligence (SIGINT) encompasses three specific collection disciplines, communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). *See* Christianson, *supra* note 219, at 39-40. COMINT refers to those activities that produce intelligence "by interception and processing of foreign communications passsed by radio, wire, or other electromagnetic means . . . and by the processing of foreign encrypted communications, however transmitted. Interception comprises search, intercept, and direction-finding. Processing

fundamental and necessary to U.S. security.[221] The NSA is the primary agency charged with the collection of foreign signals intelligence for the U.S. government.[222]

> Cryptology is vital to the U.S. intelligence community. Without the ability to decrypt enciphered communications, the value of signals intelligence activities would be diminished significantly. The history of the U.S. intelligence community, through and including operations during the Persian Gulf War, is replete with instances when the intelligence community's cryptanalytic skills provided the critical ingredient to successful U.S. military operations. Cryptology also plays a prominent role in the intelligence community's ability to meet new challenges in the post-Cold War world: the proliferation of weapons of mass destruction, terrorism, narcotics-trafficking, and economic competitiveness.[223]

The fact that strong encryption presents a threat to intelligence collection efforts, both at home and abroad, is rarely seriously questioned.[224] However, the extent the government should recognize that threat, at the expense, for example, of the software industry, has been very much at issue.[225]

---

comprises range estimation, transmitter operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plaintext, the fusion of these processes, and the reporting of the results . . . ." DESMOND BALL, SIGNALS INTELLIGENCE IN THE POST-COLD WAR ERA 122 (1993) (*quoting* U.S. National Security Council Directive no. 6, 17 Feb. 1972). COMINT is widely regarded as both the most prevalent and the most valuable intelligence. Telephone interview with high-level NSA signals intelliegence analyst (Dec. 30, 1997). While the vast majority of communications traffic is now transmitted without the use of encryption technology, that could well change if good, cheap, and fast crypto is encouraged to proliferate. *See id.*

[221] *See Report to Accompany HR 3937, Hearings on the Omnibus Export Administration Act of 1994 before the Permanent Select Committee on Intelligence,* (H.R. REP. NO. 103-531) (1994) *available at* (last visited Oct. 29, 1997) <http://www.eff.org/pub/Privacy/ITAR-export/hr3937-intell-cmte.report> [hereinafter *H.R. Rep. No.* 103-531] (commenting after receiving a thorough, classified briefing on the damaging implications of altering the present encryption control regime). *See also* Johnson, *supra* note 4, at 7 (stating that intelligence is widely considered America's "first line of defense").

[222] *See Online Encryption Technology: A Bill to Loosen Restrictions, supra* note 10 (written statement by William P. Crowell, Deputy Director, National Security Agency).

[223] *Id.*

[224] *See, e.g., Metaphor, supra* note 1, at 744-46, 850-56 (acknowleging strong crypto inhibits intelligence collection efforts but arguing nonetheless that controls on crypto are overly reliant on the exploitation of the criminal archetype).

[225] *See, e.g.,* Evans, *supra* note 93, at 490; Mark B. Hartzler, *National Security Export Controls on Data Encryption-How They Limit U.S. Competitiveness,* 29 TEXAS

Louis J. Freeh, Director of the FBI, recently stated that "the potential use of such robust encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information poses an extremely serious and, in my view, unacceptable threat to public safety."[226] The proliferation of unbreakable crypto prevents intelligence collection agencies from understanding seized files and intercepted communications.[227] Consequently, the ability of the U.S. government to thwart or later investigate dangerous criminal, terrorist, espionage, and rouge government activities is seriously and fundamentally threatened.[228]

"The intelligence community's cryptologic success depends in part on controlling the use of encryption by targets of intelligence interest. This assists in the provision of responsive, timely, and accurate intelligence support to policy-makers and the military. Controlling the dissemination of sophisticated encryption has been and will continue to be critical to those successes and U.S. national security interests."[229] If unbreakable crypto proliferates critical law enforcement and signals intelligence collection tools will be nullified.[230] There have been a number of specific cases that illustrate the significant impact proliferation presents to U.S. intelligence efforts.[231] For example, encryption to thwart intelligence collection was detected in the Aldrich Ames spy case.[232] Ramzi Yousef, alleged mastermind of the World Trade Center bombing, used encryption to protect files relating to his terrorist activities on his computer.[233] These are just two examples of a number of recent cases involving the use of crypto to thwart intelligence or law enforcement efforts.[234] "As encryption proliferates and becomes an ordinary component of mass market items, and as the strength of encryption products increases, the threat to public safety will increase proportionately."[235]

It is only by building and maintaining a strong intelligence effort,

---

INT'L L.J. 437, 440 (1994).

[226] *Pro-CODE Hearings, supra* note 58, at 13 (quoting the prepared statement of Louis J. French, Director FBI).

[227] *See id.*

[228] *See id.*

[229] *H.R. Rep. No. 103-531, supra* note 221.

[230] *See Security and Freedom Through Encryption (SAFE) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary House of Representatives,* 105th Cong. 33 (1997) (statement of Robert S. Litt, Deputy Assistant Attorney General, Criminal Division).

[231] *Id.* at 36.

[232] *Id.*

[233] *Id.* at 37.

[234] *Id.*

[235] *Id.*

including the aggressive exploitation of signals intelligence targets, that adequate warning of threats to U.S. national security can be detected and thwarted.[236] "America's emphasis on technology in the development of intelligence systems has certainly paid off handsomely. No other nation has an intelligence organization that even approaches the U.S. capability."[237] The American intelligence community has a global reach, which is a crucial and unique national security asset.[238]

Communications intelligence has never been more valuable to national security.[239] Advances in communications technology breed a corresponding increase in communications intelligence product, which in turn is accompanied by a similar growth in techniques for protecting communications, particularly cryptography.[240]

> What is not widely appreciated, however, is that despite the remarkable developments of cryptography, the communications intelligence products are now better than ever. In the recent past, there has been a migration of communications from more secure media such as wirelines or physical shipment of microwave and satellite channels; this migration has so far outstripped the application of any protective measure. Consequently, communication intelligence is so valuable that protection of its flow by keeping secret both the intelligence technology itself and techniques for protecting communication is an important objective of U.S. national

---

[236] *See* A NATIONAL SECURITY STRATEGY OF ENGAGEMENT AND ENLARGEMENT, JULY 1994, THE WHITE HOUSE. *See also* THE PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, *Science, Technology, and National Security* 6 (Dec. 1992) ("The principal threat to our future military security arises from the growing proliferation of modern weapons and associated people and technology").

[237] Bruce W. Watson, *The Future of the Intelligence Community, in* THE MILITARY INTELLIGENCE COMMUNITY 289, 290 (Gerald W. Hopple and Bruce W. Watson eds., 1989).

[238] *See* NATIONAL SECURITY STRATEGY, *supra* note 236. *See also* BALL, *supra* note 220, at 3 ("The United States maintains the most sophisticated SIGINT capabilities and operations in the world today").

[239] *See* ACM, *supra* note 91, at 22; JOHNSON, *supra* note 4, at 14 (noting that SIGINT can be the key to averting war by tipping off a belligerent's attack plans that then may be effectively countered by stepped-up diplomacy or a show of force). SIGINT, however, may also contribute to the preservation of individual American lives abroad. *Id.* "Recently a U.S. ambassador was forced to plan an evacuation because of a civil war that was spreading through the country in which he was stationed. A SIGINT intercept disclosed that a team of assassins had learned of the proposed evacuation route and intended to slay the ambassador, his wife, and children. Warned of the trap, the ambassador and his family took a different route to the airport and escaped." *Id.*

[240] *See id.* at 21-25.

security policy.[241]

2. Impact on Domestic Security as a Function of National Security

The functional and geographic separation of domestic law enforcement and intelligence ended during this last decade.[242] This occurred for the most part because of new problems with terrorism and drug trafficking and a renewed vigor on the part of the FBI to exercise their statutory authority to investigate terrorist attacks on Americans or American property, such as aircraft, wherever they may occur.[243] Controls on cryptography, consequently, became as important at home as they always have been abroad. "Strong encryption is increasingly portrayed as a threat to domestic security (public safety) and a barrier to law enforcement if it is readily available for use by terrorists or criminals."[244] Export controls, intended to prevent international proliferation of U.S. encryption technology, are consequently being joined with domestic cryptography initiatives, like key recovery proposals, and criminal penalties for use of encryption to further a crime, that seek to preserve law enforcement and signal-intelligence capabilities.[245]

Often, wiretapping can make or break a case.[246] Each year wiretaps or other electronic surveillance methods are responsible for the arrests of more than 2,000 persons, of which 20% typically end up in a conviction.[247] Stewart Baker, former General Counsel to NSA, has noted that there has already been documented cases where encryption has foiled efforts of law enforcement. The most notable case was that of a child pornographer in Santa Clara, California.[248] James Kallstrom of the FBI

---

[241] *See id.*

[242] *See* Heymann, *supra* note 210, at 4.

[243] *See id.* at 4-5.

[244] U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, ISSUE UPDATE ON INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 7 (June 1995).

[245] *See id.*

[246] *See* Seemann, *supra* note 63.

[247] *Administrative Office of the U.S. Courts. Report on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications.* Washington, D.C., Apr., 1993.

[248] *See Pro-CODE Hearings, supra* note 58, at 14 (statement of Louis J. Freeh, Director, FBI) (noting that encryption has specifically been used by a child pornographer to transmit obscene images over the Internet, within a major drug-trafficking case, and currently is being advocated by several anti-government militia groups to prevent law enforcement investigation); *see also* Seemann, *supra* note 63 (arguing that there are in fact no longer any "secret drawers" (referring to the seemingly prophetic statement of Justice Louis Brandeis that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court")

testified before a House subcommittee hearing on communications, privacy, and security that "[w]ithout the ability to effectively execute court orders for electronic surveillance, we would be unable to protect our Nation against foreign threats, terrorism, espionage, violent crime, drug trafficking, kidnapping, and other crimes."[249] For example, almost ninety percent of the narcotics leads related to money laundering came directly from domestic wiretaps.[250]

Key escrow is no doubt both an attempt to appease those who lament crypto controls and in fact an effort to strengthen the government's position relative to the proliferation of strong crypto. The primary opponents of this scheme often forcefully argue that it simply will not work because no criminal or terrorist in his or her right mind would use crypto that is escrowed.[251] However, as with many of the national security issues, the anti-escrow lobby simply misses the point.[252] Encryption is available today, but because it is neither standardized nor ubiquitous, using, buying, and distributing the crypto gear to members of the criminal conspiracy is impracticable.[253] "Up to now only a few criminals have had the resources, sophistication, and discipline to use specialized encryption systems. What worries law enforcement agencies . . . is a world where encryption is standardized and ubiquitous."[254] Such a world, that is, where anyone can get "in crypto" for a few bucks and in a matter of minutes, would be disastrous for law enforcement.[255] The idea behind the key escrow initiative is to provide strong enough crypto to meet legitimate security concerns, private and commercial, without

---

by virtue of modern technology, and therefore the only answer is encryption — strong and for all to use).

[249] *Communications and Computer Surveillance, Privacy and Security: Hearing Before the House Subcomm. on Technology, Env't and Aviation of the Comm. on Science, Space and Technology*, 103d Cong. 10 (1994) (statement of James Kallstrom, FBI) (indicating that in the ten-year period ending in 1992, more than 22,000 convictions have resulted from court-ordered electronic surveillance activity).

[250] See *Internet Security Monthly*, Feb. 1995, for remarks by Adm. Bobby Inman at MIT class, 11/21/94 (Inman was formerly a director of the NSA, Deputy Director of the CIA, and Director of Naval Intelligence).

[251] *See* Stewart Baker, *Don't Worry Be Happy, Why Clipper is Good For You*, HOTWIRED NETWORK (visited Sept. 9, 1996) <http://www.hotwired.com/wired/2.06/features/nsa.clipper.html>. Also published in WIRED, June 1994. Stewart Baker is former General Counsel of the National Security Agency. He now practices international law in Washington D.C. with Steptoe & Johnson.

[252] *Id.*

[253] *Id.*

[254] *Id.*

[255] *Id.*

"building a web of standardized encryption that shuts law enforcement agencies out."[256] In short, those criminal elements who want to avoid the escrowed-crypto used by the business world at large will have to build their own devices[257] and even then the crypto would not be able to interact with the devices used by the rest of society.[258] As one FBI agent aptly points out, "[n]obody will build secure phones just to sell to the Gambino family."[259]

Most of the attention regarding key escrow has been directed at privacy issues. Many liken "the idea of key escrow to being forced to deposit keys to your front door with the government."[260] However, once again, privacy — advocates miss the big picture. In reality, using a key escrow system will create *more* privacy safeguards from illegal law enforcement activity.[261] For example, "agents will have to satisfy the phone company that the wiretap is legitimate, *then* satisfy both custodial agencies."[262]

Key escrow is only an attempt by law enforcement to keep up with technology, not overwhelm it.[263] Clearly, law enforcement would not, as some have argued, have an open-door to intercept whatever communications they want.[264] Law enforcement would be subject to the same constitutional and statutory safeguards regarding privacy and wiretapping that now exist without escrowed encryption.[265] "It is only a device to maintain the current level of wiretapping ability law enforcement agencies

---

[256] *Id.*

[257] As they do now. *Id.*

[258] *Id.*

[259] *Id.*

[260] *See* Seemann, *supra* note 63.

[261] *Id.*

[262] *Id.* (emphasis added). *See also* Howard S. Dakoff, Note, *The Clipper Chip Proposal: Deciphering the Unfounded Fears that are Wrongfully Derailing its Implementation,* 29 J. MARSHALL L. REV. 475, 497-98. The article concludes that key escrow "will not provide the government with any more power to pry into individual private lives than the current system for wiretapping provides. It is only a device to maintain the current level of wiretapping ability law enforcement agencies have at their disposal." *Id.* at 498.

[263] *See id.* at 493-97 (discussing the law enforcement and escrowed encryption controversy).

[264] *See id.* at 494-96 (discussing how Title III would apply to communications intercepted with a clipper chip and, thus, limit the government's ability to intercept communications).

[265] *See id.* at 491-94 (describing the Title III standards which must be met for an intercept of communications to be constitutional).

have at their disposal. The Clipper Chip is not Orwellian;[266] it is merely a product of the evolution of the Technological Age."[267]

C. Crypto Anarchy?

> A specter is haunting the modern world, the specter of crypto anarchy . . . [j]ust as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions.[268]

The term "crypto anarchy" was coined several years ago by a group techno-anarchists.[269] As its catchy name suggests, it envisions a *Brave New World* in which governments disintegrate and individuals form the nucleus of society, without, of course, all forms of government interference.[270] Proponents, most vocally, Tim May,[271] argue that crypto anarchy is an inevitable, and of course desirable, outcome of the proliferation of public key crypto.[272] "With this technology, they say, it will be impossible for governments to control information, compile dossiers, conduct wiretaps, regulate economic arrangements, and even collect taxes. Individuals will be liberated from coercion by their physical neighbors and by governments."[273] But is this such a good thing?

Surprisingly, even Tim May, the apparent leader of the movement, acknowledges the apparent danger of widespread availability of unbreakable crypto.[274] He, however, tends to embrace it rather than fear it. With government essentially locked out, "computers and telecommunications systems would become safe havens for criminal activity . . . [providing]

---

[266] *See* GEORGE ORWELL, 1984 5 (1949) ("Big Brother is watching you").

[267] Dakoff, *supra* note 193, at 498.

[268] Timothy C. May, *The Crypto Anarchist Manifesto, reprinted in* HIGH NOON ON THE ELECTRONIC FRONTIER 237 (1996) [hereinafter *Manifesto*].

[269] *See generally* Timothy C. May, *Cyphernomicon* (visited Nov. 2, 1997) <http://swiss.ai.mit.edu/6805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ>[hereinafter *Cyphernomicon*] (outlining the history of the cyperpunks and crypto anarchy movements).

[270] *Id.* ¶ 16.4.2.

[271] *See, e.g.*, Timothy C. May, *Crypto Anarchy and Virtual Communities* (visited Oct 26, 1997) <http://www.powergrid.com/1.01/cryptoanarchy-wp.html#8a>.

[272] *See id.*

[273] Dorothy Denning, *The Future of Cryptography* (last modified Jan. 6, 1996) <http://guru.cosc.georgetown.edu/~denning/crypto/Future.html> [hereinafter *Future of Crypto*] (arguing that key escrow should be the new paradigm of cryptography, not crypto anarchy).

[274] *See Cyphernomicon, supra* note 269 ¶ 11.4.4.

a means for tax evasion, money laundering, espionage (with digital dead drops), contract killings, and implementation of data havens for storing and marketing illegal or controversial material."[275] To argue that national security would be in jeopardy from such a scenario would clearly be an understatement. The proliferation of strong crypto would solve the problem of confidentiality for companies and individuals worldwide, but we have to ask ourselves, at what cost?[276] As May writes:

> The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.[277]

Ultimately, crypto anarchy is an international threat, brought on by the proliferation of strong crypto. Denning strongly advocates an international approach to the problem of crypto anarchy.[278] Such an approach would have to provide for both secure transnational communications and sufficient means for electronic surveillance of criminal and terrorist activity by governments.[279] "Key escrow has emerged as one approach that can meet the confidentiality and data recovery needs of organizations while allowing authorized governments access to fight terrorism and crime."[280]

VI. CONCLUSION

> It may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.[281]
>
> – Edgar Allen Poe[282]

---

[275] *See Future of Crypto, supra* note 273.

[276] *See id.*

[277] *See Manifesto, supra* note 268.

[278] *Id.*

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

[280] *Id.*

[281] EDGAR ALLEN POE, *A Few Words on Secret Writing, in* ESSAYS AND MISCELLANIES (James A. Harrison ed., 2d ed. 1979).

[282] Edgar Allen Poe was an amateur cryptographer of some regard, among other things. *See* ANDRE BACARD, THE COMPUTER PRIVACY HANDBOOK 73 (1995). *See also* Daniel W. Dukes, *The Legend of Poe the Cryptographer* (visited Nov. 16, 1997)

Cryptography has been and largely still is an enigma to the vast majority of the world. Rapid advances in computers and other related technology, however, have forced many of the leading governments of the world to not only try to understand the new technology now guiding this centuries-old "secret writing" but sort through the multitude of complex, diverse, and often emotionally charged issues that cryptography engenders. This by no means amounts to a simple wave of a magic wand, especially in the United States, whose very fabric of existence as a democratic state is predicated on broad notions of personal privacy and free speech. However, hard choices must be made. Unfortunately, every time the United States has a lasting peace, it becomes complacent about security and overly focused on economic growth. History, however, has repeatedly admonished the United States that such a mistake may have mortal ramifications.

There are, no doubt, shortcomings in prior efforts to control the proliferation of crypto, most notably the confusing and contradictory ITAR. That alone is not a sufficient reason to dismantle the entire apparatus, as some have suggested. A viable threat to national security exists; it is not simply smoke and mirrors. It is as absurd to assert, as opponents to crypto controls often do, that there is no threat because the government cannot empirically, definitively demonstrate it, as it is for the government to merely state in a perfunctory manner that there is a threat, "trust us." Both sides must give a little. Within a very short time the power to control information, for good or evil, will be unparalleled in world history. It may well become the ultimate power.

In this now technologically rich world it is unlikely if not impossible to entirely confine the effect of export controls to locations purely abroad, or to only select locations of the world. Fallout is natural, yet should not be a subterfuge for complete decontrol. Like most things in American

---

<http://www.nadn.navy.mil/EnglishDept/poeperplex/cryptop.htm> (describing Poe's efforts to mix his interest in cryptography with his writing); CODEBREAKERS, *supra* note 21, at 783-93 (comprehensively detailing Poe's contributions to the craft of cryptography and noting that Poe's story, "*The Gold-Bug* remains unequalled as a work of fiction turning upon a secret message"). "That the early American writer should have become interested in cryptology seems almost inevitable. He urged exactness in thinking, talked about "ratiocination," and wrote stories, like *The Purloined Letter*, that demanded a methodical logic. But he also wrote poems of an unearthly beauty and the macabre *Tales of the Grotesque and Arabesque*, and he looked into such irrational subjects as mesmerism and phrenology. Cryptology, more than other subjects, is split the same way. It beams the hard bright searchlight of reason upon the phenomena it investigates. At the same time it glimmers with the pale, eerie, indistinct moonshine of mysticism and spooky powers." *Id.* at 783.

politics, issues are measured in extremes. Fortunately, this political methodology of "extreme advocacy" has generally contributed toward moving this country toward a balanced, prudent, and middle ground on all issues. Cryptography should fair no differently. A middle ground must be sought.

Complete decontrol of crypto is insane. Complete control is equally insane. Key escrow, escrowed encryption, or key recovery then becomes the "key" to national security. Hyperbole aside, escrowed encryption is unlikely to be a serious attempt by the government to "back-door Big Brother." Because if it were, the government has really gone about it in all the wrong manner. One could only surmise, given the technologically-advanced intelligence apparatus that the United States indisputably possesses, that there must be easier and less "public" ways to spy on mom and her apple pie.

Escrowed encryption appears to be an attempt to maintain the status quo, not one-up-it. Escrowed encryption allows a limited proliferation of strong crypto to those who desperately need it, but without seriously compromising security. Export controls limit the availability of U.S.-made crypto, much like export controls limit the availability of Patriot Missile technology despite similar systems being available to one degree or another worldwide. Additionally, "[k]ey escrow is a technology that offers tools that would assure no individual absolute privacy or untraceable anonymity in all transactions . . . [allowing] individuals to choose civil society over an anarchistic one."[283] The government is charged with the awesome and, per se, speculative job of protecting the security of this country. To err on the side of being *too conservative* with the control of a potentially dangerous technology is, in fact, reasonable and in all likelihood the preferred choice of most Americans.

"National security" is a nebulous concept and should be challenged.[284] But it also must be respected if a legitimate threat is presented. It is not, despite the invective, an either/or proposition (that is, constitutional rights versus security; economic growth versus security, etc.). All interests, from privacy and free speech to security and economics must be respected and a policy on the control of strong crypto must be a balance of their respective needs.

This Note as a whole makes a relatively simple statement: do not misunderstand or underestimate the national security interest in controlling strong crypto. It is vital; it is significant; and it compels respect.

---

[283] *See Future of Cryptography, supra* note 273.

[284] To be sure, the invocation of "national security" has been abused in the past; however, that does not, and should not, foreclose all future invocations. That would be plainly unreasonable and, moreover, extremely dangerous.